

**Austria: Detailed Assessment Report on Anti-Money Laundering  
and Combating the Financing of Terrorism**

This Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism for Austria was prepared by a staff team of the International Monetary Fund using the assessment methodology adopted by the Financial Action Task Force in February 2004 and endorsed by the Executive Board of the IMF in March 2004. The views expressed in this document are those of the staff team and do not necessarily reflect the views of the Government of or the Executive Board of the IMF.

**To assist the IMF in evaluating the publication policy, reader comments are invited and may be sent by e-mail to [publicationpolicy@imf.org](mailto:publicationpolicy@imf.org).**

Copies of this report are available to the public from

International Monetary Fund • Publication Services  
700 19th Street, N.W. • Washington, D.C. 20431  
Telephone: (202) 623 7430 • Telefax: (202) 623 7201  
E-mail: [publications@imf.org](mailto:publications@imf.org) • Internet: <http://www.imf.org>

Price: \$18.00 a copy

**International Monetary Fund  
Washington, D.C.**

**AUSTRIA**

**DETAILED ASSESSMENT  
REPORT ON ANTI-MONEY  
LAUNDERING AND  
COMBATING THE FINANCING  
OF TERRORISM**

**JUNE 2009**

INTERNATIONAL MONETARY FUND  
LEGAL DEPARTMENT

Contents		Page
Acronyms .....		6
Preface .....		9
Executive Summary .....		10
1.	General .....	16
1.1	General Information on Austria .....	16
1.2	General Situation of Money Laundering and Financing of Terrorism .....	19
1.3	Overview of the Financial Sector and DNFBP .....	21
1.4	Overview of commercial laws and mechanisms governing legal persons and arrangements .....	30
1.5	Overview of the Strategy to Prevent Money Laundering and Financing of Terrorism .....	31
2.	Legal System and Related Institutional Measures .....	37
2.1	Criminalization of Money Laundering (R.1 & 2) .....	37
2.1.1	Description and Analysis .....	37
2.1.2	Recommendations and Comments .....	49
2.1.3	Compliance with Recommendations 1 & 2 .....	49
2.2	Criminalization of Terrorist Financing (SR.II) .....	49
2.2.1	Description and Analysis .....	49
2.2.2	Recommendations and Comments .....	55
2.2.3	Compliance with Special Recommendation II .....	55
2.3	Confiscation, freezing and seizing of proceeds of crime (R.3) .....	56
2.3.1	Description and Analysis .....	56
2.3.2	Recommendations and Comments .....	65
2.3.3	Compliance with Recommendation 3 .....	65
2.4	Freezing of funds used for terrorist financing (SR.III) .....	65
2.4.1	Description and Analysis .....	65
2.4.2	Recommendations and Comments .....	75
2.4.3	Compliance with Special Recommendation III .....	75
2.5	The Financial Intelligence Unit and its Functions (R.26) .....	76
2.5.1	Description and Analysis .....	76
2.5.2	Recommendations and Comments .....	86
2.5.3	Compliance with Recommendation 26 .....	87
2.6	Law enforcement, prosecution and other competent authorities—the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R. 27 & 28) .....	87
2.6.1	Description and Analysis .....	87
2.6.2	Recommendations and Comments .....	93
2.6.3	Compliance with Recommendations 27 & 28 .....	94
2.7	Cross Border Declaration or Disclosure (SR.IX) .....	94
2.7.1	Description and Analysis .....	94
2.7.2	Recommendations and Comments .....	100
2.7.3	Compliance with Special Recommendation IX .....	101
3.	Preventive Measure—Financial Institutions .....	101
3.1	Risk of Money Laundering or Terrorist Financing .....	102
3.2	Customer Due Diligence, Including Enhanced or Reduced Measures (R.5 To 8) .....	102

	3.2.1	Description and Analysis .....	102
	3.2.2	Recommendations and Comments .....	128
	3.2.3	Compliance with Recommendations 5 to 8.....	129
3.3		Third Parties And Introduced Business (R.9).....	130
	3.3.1	Description and Analysis .....	130
	3.3.2	Recommendations and Comments .....	132
	3.3.3	Compliance with Recommendation 9 .....	132
3.4		Financial Institution Secrecy or Confidentiality (R.4) .....	132
	3.4.1	Description and Analysis .....	132
	3.4.2	Recommendations and Comments .....	136
	3.4.3	Compliance with Recommendation 4 .....	137
3.5		Record-Keeping and Wire Transfer Rules (R.10 & SR.VII) .....	137
	3.5.1	Description and Analysis .....	137
	3.5.2	Recommendations and Comments .....	141
	3.5.3	Compliance with Recommendation 10 and Special Recommendation VII .....	142
3.6		Monitoring of Transactions and Relationships (R.11 & 21) .....	142
	3.6.1	Description and Analysis .....	142
	3.6.2	Recommendations and Comments .....	144
	3.6.3	Compliance with Recommendations 11 & 21 .....	145
3.7		Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 & SR.IV)..	146
	3.7.1	Description and Analysis .....	146
	3.7.2	Recommendations and Comments .....	154
	3.7.3	Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV .....	155
3.8		Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22) .....	156
	3.8.1	Description and Analysis .....	156
	3.8.2	Recommendations and Comments .....	161
	3.8.3	Compliance with Recommendations 15 & 22 .....	161
3.9		Shell Banks (R.18) .....	162
	3.9.1	Description and Analysis .....	162
	3.9.2	Recommendations and Comments .....	162
	3.9.3	Compliance with Recommendation 18 .....	162
3.10		The Supervisory and Oversight System—Competent Authorities and SROs. Role, Functions, Duties, and Powers (Including Sanctions) (R.23, 29, 17 & 25) .....	162
	3.10.1	Description and Analysis .....	162
	3.10.2	Recommendations and Comments .....	181
	3.10.3	Compliance with Recommendations 17, 23, 25 & 29 .....	182
3.11		Money or Value Transfer Services (SR.VI) .....	183
	3.11.1	Description and Analysis .....	183
	3.11.2.	Recommendations and Comments .....	184
	3.11.3	Compliance with Special Recommendation VI .....	184
4.		Preventive Measures—Designated Non-Financial Businesses And Professions.....	184
4.1		Customer Due Diligence and Record-keeping (R.12).....	186
	4.1.1	Description and Analysis .....	186
	4.1.2.	Recommendations and Comments .....	206
	4.1.3.	Compliance with Recommendation 12 .....	208
4.2		Suspicious Transaction Reporting (R.16).....	210
	4.2.1	Description and Analysis .....	210
	4.2.2.	Recommendations and Comments .....	218
	4.2.3.	Compliance with Recommendation 16 .....	219

4.3	Regulation, Supervision, and Monitoring (R.24-25).....	219
4.3.1	Description and Analysis .....	219
4.3.2	Recommendations and Comments .....	229
4.3.3	Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP) .....	229
4.4	Other Non-Financial Businesses and Professions—Modern-Secure Transaction Techniques (R.20) .....	230
4.4.1	Description and Analysis.....	230
4.4.2	Recommendations and Comments .....	231
4.4.3	Compliance with Recommendation 20 .....	231
5.	Legal Persons And Arrangements and Non-Profit Organizations.....	231
5.1	Legal Persons—Access to Beneficial Ownership and Control Information (R.33).....	231
5.1.1	Description and Analysis .....	231
5.1.2	Recommendations and Comments .....	239
5.1.3	Compliance with Recommendation 33 .....	240
5.2	Legal Arrangements—Access to Beneficial Ownership and Control Information (R.34).....	240
5.2.1	Description and Analysis .....	240
5.2.2	Recommendations and Comments .....	243
5.2.3	Compliance with Recommendation 34 .....	243
5.3	Non-Profit Organizations (SR. VIII).....	243
5.3.1	Description and Analysis .....	243
5.3.2	Recommendations and Comments .....	249
5.3.3	Compliance with Special Recommendation VIII.....	249
6.	National And International Cooperation .....	250
6.1	National Cooperation and Coordination (R.31 & R. 32).....	250
6.1.1	Description and Analysis .....	250
6.1.2	Recommendations and Comments .....	252
6.1.3	Compliance with Recommendations 31 & 32.....	252
6.2	The Conventions and UN Special Resolutions (R.35 & SR.I).....	252
6.2.1	Description and Analysis .....	252
6.2.2	Recommendations and Comments .....	254
6.2.3	Compliance with Recommendation 35 and Special Recommendation I ...	255
6.3	Mutual Legal Assistance (R.36-38, SR.V).....	255
6.3.1	Description and Analysis .....	255
6.3.2	Recommendations and Comments .....	261
6.3.3	Compliance with Recommendations 36 to 38 and Special Recommendation V.....	262
6.4	Extradition (R.37, 39, SR.V).....	263
6.4.1	Description and Analysis .....	263
6.4.2	Recommendations and Comments .....	267
6.4.3	Compliance with Recommendations 37 & 39, and Special Recommendation V.....	267
6.5	Other Forms of International Cooperation (R.40 & SR.V).....	267
6.5.1	Description and Analysis .....	267
6.5.2	Recommendations and Comments .....	275
6.5.3	Compliance with Recommendation 40 and Special Recommendation V ...	275
7.	Other Issues .....	276
7.1	Resources and Statistics .....	276

## Tables

1. Ratings of Compliance with FATF Recommendations.....	277
2. Recommended Action Plan to Improve the AML/CFT System.....	289

## Statistical Tables

1. Categories of Financial Institutions.....	23
2. Market shares of Austrian banks in CESE and CIS countries.....	23
3. Credit institutions (December 31, 2007).....	24
4. Domestic Financial Institutions.....	24
5. Financial Activities Listed in the Glossary of the 40 Recommendations.....	25
6. Activity of Casinos in Austria.....	27
7. Real Estate Activity in Austria.....	28
8. Predicate offenses in Austria.....	39
9. Money Laundering Cases.....	45
10. Statistic of Convictions for Serious Offenses.....	46
11. Statistics on persons under investigation for the designated categories of offenses referred to by	46
12. ML-Convictions 2004 – 2007.....	48
13. ML-Convictions 2004–2007.....	48
14. ML Offenses (Article 165 StGB).....	64
15. Interim injunctions by court order applied for by the A-FIU.....	64
16. Reporting Entities.....	77
17. FIU Functions.....	80
18. Authorities competent for investigating STRs.....	82
19. STRs Received by the A-FIU.....	85
20. ML-Related STRs.....	85
21. FT-Related STRs.....	86
22. Cases submitted to the Prosecutor.....	86
23. Statistics Cash Control Austria.....	95
24. Origin of STRs.....	147
25. STRs investigated by the BVT.....	149
26. Onsite Examinations of Credit Institutions.....	164
27. Supervisory Actions related to AML/CFT Infringements.....	176
29. Acts implementing AML/CFT measures for DNFBPs.....	185
30. STRs filed by DNFBPs.....	213
31. AML/CFT Regulation and Supervision of DNFBPs.....	220
32. Legal Frameworks for NPOs.....	247
33. Providers of information to the A-FIU.....	251
34. Information received/sent through the ESW.....	274
35. Breakdown of information requested by foreign FIUs.....	274

## Annexes

Annex 1. Authorities' Response to the Assessment.....	300
Annex 2. Details of All Bodies Met During the On-Site Visit.....	301
Annex 3. List of All Laws, Regulations, and Other Material Received.....	302
Annex 4 Copies of Key Laws, Regulations, and Other Measures.....	304

## ACRONYMS

ABGB	Civil Code ( <i>Allgemeines Bürgerliches Gesetzbuch</i> )
A-FIU	Austrian Financial Investigation Unit
AHG	Public Liability Act ( <i>Amtshaftungsgesetz</i> )
AktG	Stock Corporation Act ( <i>Aktiengesetz</i> )
AML	Anti-Money Laundering and Combating the Financing of Terrorism
ARHG	Law on Extradition and Mutual Assistance ( <i>Auslieferungs- und Rechtshilfegesetz</i> )
AVG	General Administrative Procedure Act ( <i>Allgemeines Verwaltungsverfahrensgesetz</i> )
BKA	Criminal Intelligence Service ( <i>Bundeskriminalamt</i> )
BKA-G	Criminal Intelligence Service Act ( <i>Bundeskriminalamtgesetz</i> )
BiBu-ARL	Directive on the Practice of the Accountancy Professions ( <i>Bilanzbuchhaltungs- (Berufs) Ausübungsrichtlinie</i> )
BiBuG	Accountancy Act ( <i>Bilanzbuchhaltungsgesetz</i> )
BörseG	Stock Exchange Law ( <i>Börsegesetz</i> )
B-VG	Federal Constitutional Law ( <i>Bundes-Verfassungsgesetz</i> )
BVT	Federal Agency for State Protection and Counter-Terrorism ( <i>Bundesamt für Verfassungsschutz und Terrorismusbekämpfung</i> )
BWG	Banking Act ( <i>Bankwesengesetz</i> )
CASAG	Casinos Austria Aktiengesellschaft
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CESE	Central, Eastern and Southeastern Europe
CFT	Combating the Financing of Terrorism
CIS	Community of Independent States
DevG	Foreign Exchange Act ( <i>Devisengesetz</i> )
DNFBP	Designated Non-Financial Businesses and Professions
DSt	Disciplinary Statute for lawyers and lawyer-candidates ( <i>Disziplinarstatut</i> )
ECB	European Central Bank
EEA	European Economic Area
EU	European Union
EU-JZG	Federal law on judicial cooperation in criminal matters with EU Member States ( <i>Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union</i> )
FATF	Financial Action Task Force
FBG	Commercial Register Act ( <i>Firmenbuchgesetz</i> )
FinStrG	Fiscal Penal Code ( <i>Finanzstrafgesetz</i> )
FMA	Financial Market Authority
FMABG	Financial Market Authority Act ( <i>Finanzmarktaufsichtsbehördengesetz</i> )
FSAP	Financial Sector Assessment Program
FT	Financing of terrorism
GDP	Gross Domestic Product
GewO	Trade Act ( <i>Gewerbeordnung</i> )
GRECO	Groupe d'Etats contre la Corruption
GSpG	Gambling Law ( <i>Glücksspielgesetz</i> )

ICSFT	International Convention for the Suppression of the Financing of Terrorism
LEG	Legal Department of the IMF
LVT	States' Agencies for Protection and Counter-Terrorism ( <i>Landesämter für Verfassungsschutz</i> )
MIFID	EU's Markets In Financial Instruments Directive
ML	Money Laundering
MLA	Mutual Legal Assistance
MoE	Federal Ministry of Economy, Family and Youth
MoF	Federal Ministry of Finance
MoFA	Federal Ministry for European and International Affairs
MoI	Federal Ministry of the Interior
MoJ	Federal Ministry of Justice
MOU	Memorandum of Understanding
MVT	Money Value Transfer
NCCT	Non Cooperative Countries and Territories
NO	Notaries' Act
NPO	Nonprofit organization
OECD	Organization for Economic Development and Cooperation
OeNB	Austrian National Bank ( <i>Oesterreichische Nationalbank</i> )
OFAC	US Treasury Office of Foreign Assets Control
PEP	Politically-Exposed Person
PolKG	Police Cooperation Act ( <i>Polizeikooperationsgesetz</i> )
RAO	Lawyer's Act ( <i>Rechtsanwaltsordnung</i> )
ROSC	Report on Observance of Standards and Codes
SPG	Security Police Act ( <i>Sicherheitspolizeigesetz</i> )
SPOC	Single Point Of Contact
SRO	Self-Regulatory Organization
StGB	Criminal Code ( <i>Strafgesetzbuch</i> )
StPO	Code of Criminal Procedure ( <i>Strafprozessordnung</i> )
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
TFC	Terrorist Financing Convention
UGB	Commercial Code ( <i>Unternehmensgesetzbuch</i> )
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution
US	United States
VAG	Insurance Supervision Act ( <i>Versicherungsaufsichtsgesetz</i> )
VerG	Associations Act ( <i>Vereinsgesetz</i> )
WAG	Securities Supervision Act ( <i>Wertpapieraufsichtsgesetz</i> )
VbVG	Statute on the Responsibility of Entities for Criminal Offenses ( <i>Verbandsverantwortlichkeitsgesetz</i> )
VStG	Administrative Penal Act ( <i>Verwaltungsstrafverfahrensgesetz</i> )
VwGG	Administrative Court Act ( <i>Verwaltungsgerichtshofgesetz</i> )
VwGH	Administrative Court ( <i>Verwaltungsgerichtshof</i> )
WKO	Austrian Federal Economic Chamber ( <i>Wirtschaftskammern Österreichs</i> )

WT-ARL	Directive on the Practice of the Chartered Public Accountants and Tax Consultants Professions ( <i>Wirtschaftstreuhänderberufs-Ausübungsrichtlinie</i> )
WTBG	Act on the Profession of Chartered Public Accountants and Tax Consultants ( <i>Wirtschaftstreuhänderberufsgesetz</i> )
ZollR-DG	Customs Law ( <i>Zollrechts-Durchführungsgesetz</i> )
ZVR	Central Register of Associations ( <i>Zentrales Vereinsregister</i> )

## PREFACE

This assessment of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of Austria is based on the 40 Recommendations 2003 and the 9 Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT assessment Methodology 2004, as updated in February 2008. The assessment team considered all the materials supplied by the authorities, the information obtained on site during their mission from September 15–30, 2008, and other verifiable information subsequently provided by the authorities. During the mission, the assessment team met with officials and representatives of all relevant government agencies and the private sector. A list of the bodies met is set out in Annex 2 to the detailed assessment report.

The assessment was conducted by a team of assessors composed of staff of the International Monetary Fund (IMF) and one expert acting under the supervision of the IMF. The evaluation team consisted of: Alain Védrenne-Lacombe (LEG, team leader); Nadine Schwarz, Giuseppe Lombardo, Emmanuel Mathias (LEG); and Helen Hatton (LEG expert, Deputy Director General, Jersey Financial Services Commission). The assessors reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter and punish money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs). The assessors also examined the capacity, implementation, and effectiveness of all these systems.

This report provides a summary of the AML/CFT measures in place in Austria at the time of the mission or shortly thereafter. It describes and analyzes those measures, sets out Austria levels of compliance with the FATF 40+9 Recommendations (see Table 1) and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

The assessors would like to express their gratitude to the Austrian authorities for their support and cooperation and for the high standard of organization throughout the assessment mission.

## EXECUTIVE SUMMARY

### Key Findings

1. The crime level in Austria is among the lowest in EU Member States, and the authorities consider that the country's exposure to money laundering and financing of terrorism risks is limited. However, due to its geographical location and its historical ties with Central Eastern and Southern Europe countries, Austria may be used by foreign criminal organizations as a transit point for drugs and other trafficking, as well as a destination for criminal money, attracted by its reputation for political stability, tradition of banking secrecy, and attractive tax regime.
2. The authorities have designed and are implementing a comprehensive AML/CFT system, supported by well-developed federal administrative and supervisory bodies, and active professional organizations.
3. Criminalization of money laundering is generally in line with the FATF standards, and the legal framework provides for a wide range of confiscation and provisional measures. However, the small number of convictions for money laundering, low legal penalties and low amounts of proceeds of crime confiscated raise questions about the overall effectiveness of the system. Criminal provisions for the financing of terrorism, although largely consistent with the 1999 Convention, do not cover the full range of activities covered by the FATF standard.
4. The transposition of the Third EU AML Directive resulted in a large overhaul, expansion and strengthening of the Austrian AML/CFT regime which now covers the broadest range of financial activities and non-financial businesses and professions, except certain casinos. However, some provisions should be brought more closely into line with the FATF standard, and overall, more time is needed before all requirements are fully implemented.
5. The supervisory system for financial institutions is generally sound and efficient. Licensing requirements and the regime of sanctions need to be strengthened, and additional resources should be allocated to supervisory bodies.
6. The Austrian Financial Investigation Unit (A-FIU) is an effective police unit, but it does not fulfil the suspicious transactions report (STR) analysis and dissemination functions of an FIU. The possibility that information on the person making an STR may be disclosed to the defendant pursuant to a criminal procedure may be contributing to the overall low level of reporting.
7. Legal provisions and jurisprudence provide gateways for the authorities to obtain data protected by banking secrecy, but requests by public prosecutors are subject to restrictive conditions that financial institutions and legal professions may exploit to decline to supply information.
8. While the system of registration of legal persons is generally well-developed, access to beneficial ownership data on some non-profit organizations, legal arrangements (*Treuhand*) and some legal persons, notably foundations and companies issuing bearer shares, is hindered.
9. Various *fora* have been established to ensure national cooperation and coordination. The deficiencies noted in the domestic legal framework slow down the provision of mutual legal assistance.

## Legal System and Related Institutional Measures

10. The provisions which criminalize money laundering in Austria closely follow the Vienna and Palermo Conventions. The offense of money laundering extends to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime, and irrespective of the place where the predicate offense was committed. Predicate offenses include all serious offenses under Austrian criminal law, which cover all categories of offenses designated by the FATF, as well as a wide range of misdemeanors, with the exception of counterfeiting and piracy of products. It was not established that the non-criminalization of self-laundering is supported by fundamental principles according to the FATF standard.

11. The liability of natural persons is broader than required by the Conventions, and the general criminal liability has been enlarged to include legal persons and entities for all penal offenses.

12. The criminalization of the financing of terrorism is consistent with the 1999 UN Terrorist Financing Convention, and addresses all activities, without considering the place where the offense was committed. However, it needs to be extended further to include in full the financing of terrorist organizations and individual terrorists, regardless of the use of the funds provided.

13. Prosecutorial units specialized in financial crime prosecution have been set up, and investigations are generally conducted by specific police units, the A-FIU for money laundering cases, and the Federal Agency for State Protection and Counter-Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*; BVT) for terrorist financing cases.

14. The overall legal framework is fairly comprehensive, but questions remain regarding its effective implementation. Few convictions for money laundering have been obtained compared to the number of convictions for predicate offenses, in particular drug-related offenses, which are subject to investigations and convictions. Elements contributing to a smaller number of money laundering cases appear to be the non-criminalization of self-laundering, practical difficulties in establishing a link with a predicate offense, especially when those offenses are committed abroad, and prosecutors' practice of indicting money laundering under "participation" in the predicate offense. There were no convictions for FT between 2004 and 2007. Moreover, the AML/CFT sanction regime applicable to natural and legal persons needs to be strengthened further.

15. The legislation provides for a wide range of confiscation and provisional measures which apply to property that has been laundered or constitutes proceeds of any money laundering, financing of terrorism or other predicate offenses. The mechanism applies to all property items in Austria, as well as to property of corresponding value. However, restrictive conditions to law enforcement's access to information and documents held by financial institutions and some designated non-financial businesses and professions (DNFBPs) limit its overall effectiveness. The legal regime for non-conviction based forfeiture of assets held by a criminal organization or a terrorist group is extensive, but has not been applied yet.

16. Measures to freeze funds or other assets of terrorists, those who finance terrorism and terrorist organizations are mainly implemented in Austria by European Council Regulations, which are directly applicable, and Council Common Positions which are enacted through Official Announcements of the Austrian National Bank (*Oesterreichische Nationalbank*, OeNB). However,

the execution of directly applicable EU regulations presents some difficulties in regard to the freezing of non-financial assets, and there is also a need for additional guidance for the private sector on the freezing obligation.

17. Pursuant to their relevant laws and regulations, financial institutions and DNFBPs report suspicious activities to a unit of the Federal Criminal Police Department, the A-FIU. It receives STRs from reporting entities, which are dealt with in the same way as criminal complaints, and conducts criminal investigations, with full investigative powers and access to information. The A-FIU does not perform two major functions required for an FIU by the international standard, i.e., analysis and dissemination of information. Moreover, the A-FIU is not responsible for FT cases, which fall within the responsibility of the BVT. The A-FIU maintains regular contact with reporting entities, providing general guidance and specific advice and feedback. This approach offers opportunities for efficient exchange of information.

18. The banking legislation sets out strict banking secrecy provisions, but legal provisions and jurisprudence provide gateways for the authorities to access protected information. Requests for information made to financial institutions by the A-FIU acting on the basis of STRs are usually complied with, but court orders requested by the office of public prosecution are rejected if requests, in the view of financial institutions, do not provide substantive, material and adequate evidence that the legal conditions for disclosure are met, thus delaying access to information.

### **Preventive Measures-Financial Institutions**

19. Since Austria's last evaluation, several measures have been taken to improve the overall AML/CFT framework: subsequent legislative and regulatory revisions and the implementation of the Third EU ML Directive resulted in a large overhaul, expansion and strengthening of the AML/CFT regime.

20. All persons and entities who conduct as a business in Austria one or more of the financial activities listed in the FATF definition of "financial institution" are subject to AML/CFT measures, which are set out in sector-specific laws. Following the transposition of the Third EU ML Directive, additional have been incorporated into the Austrian legal framework relating to customer identification, the definition of beneficial ownership and the identification and monitoring of politically exposed persons (PEPs) and cross-border correspondent banks. A good level of implementation was found not only in large international financial firms, but also in smaller financial institutions, in particular with respect to AML/CFT measures that have been in place for some years. However, the effective implementation of some new provisions, which came into force on January 1, 2008, could not be fully established, and some operational circulars are still pending.

21. Overall, the measures set out in the financial sector laws are generally in line with the FATF Recommendations. Customer due diligence (CDD) requirements have been expanded and cover all customers and beneficial owners, whether natural or legal persons. They should nevertheless be expanded further by removing three exemptions, and requiring additional CDD for beneficiaries of some smaller savings deposit accounts. Financial institutions have developed and implemented strict selection procedures at the inception of business relationships, notably when they rely on intermediaries or third-parties to perform elements of the CDD process.

22. The revised legislation introduces a risk-based approach to CDD modeled on the provisions of the EU Directive. It requires financial institutions to conduct a risk-analysis of their business, apply risk-based CDD, and take appropriate measures to address higher risk situations. Financial institutions have initiated important programs to acquire and develop IT tools which are required to implement risk-sensitive monitoring. The authorities should consider conducting a ML/FT risk assessment to establish whether additional legal provisions are required to mitigate risks specific to Austria, such as bearer shares, personal asset holding vehicles, and private banking.

23. The legislation also calls for enhanced due diligence for specific risks singled out by the FATF standard, in particular non-face-to-face business, cross-border correspondent banking, and business with PEPs. However, the nature and scope of monitoring measures are not defined, but rather fall within the ambit of the risk-based approach, and are thus left to the discretion of financial institutions. Moreover, financial institutions should be specifically required to examine the background and purpose of transactions they view as unusual and record their findings in writing. The general requirement to maintain CDD records is fully in line with the standard.

24. Most of the STRs originate from “credit institutions” (which, in Austria, covers a number of financial institutions as defined in the standard in addition to banks), especially money transfer services. Pursuant to the criminal procedure, information may be disclosed to the defendant, after criminal proceedings have been initiated. Such disclosure may be a contributing factor to the overall level of reporting which, in Austria, is low. In November 2008, the authorities initiated an action plan for better protecting the anonymity of reporting entities and persons filing STRs.

25. Most categories of financial institutions are subject to broad obligations regarding the compliance management and internal audit functions, but these requirements need better focus to ensure adequate and comprehensive coverage of exposure to ML/FT risks. The compliance officer’s seniority, independence and right to access CDD information, transaction records and other relevant information should be set out in the law.

26. The Financial Market Authority (FMA) has the overall responsibility for regulation, supervision and enforcement in the financial sector, but since January 2008, the OeNB has been entrusted with conducting offsite monitoring and onsite examinations of banks. The broad definition of banking activities subjects a wide range of institutions to supervision, and includes notably money value transfer services that can only be conducted by credit institutions. The licensing requirements and supervisory process would prohibit the establishment and operation of shell banks. However, there are concerns about the adequacy of the licensing process, especially in regard to the assessment of significant or controlling interests when the capital of a financial institution is in form of bearer shares. Fit and proper tests should also be applied to senior managers and all supervisory board members.

27. The increasing number of examinations, as well as meetings with senior management of supervised entities demonstrates that the FMA and the OeNB are taking steps to ensure closer AML/CFT supervision. Both authorities rely on external auditors to examine regularly all financial institutions, and confirm that AML/CFT controls are in place and operational. The capacity of both the FMA and the OeNB needs further strengthening and additional resources are required to enable their respective supervisory divisions to step up the number of onsite examinations and to cover all areas of ML/FT risk. The sanctioning regime does not appear to be sufficiently proportionate and

dissuasive. In addition, the application of sanctions should be extended to all members of supervisory boards and senior management.

28. Local district authorities supervise domestic financial institutions that carry limited specialized financial business. The legal provisions, that regulate the licensing, business, supervision and sanctioning of these institutions, are not sufficiently adapted to their activity and ML/FT risks.

### **Preventive Measures-Designated Non-Financial Businesses and Professions**

29. Further to the Third EU AML Directive, all DNFBPs are covered in laws and regulations, and the range of covered activities goes beyond the FATF standard to include all types of dealers, auctioneers and accounting professions. However, the preventive measures applicable to these businesses and professions need to be expanded and better tailored to their specificities. CDD requirements should be defined for all casinos operating in Austria, including internet casinos, while some legal ambiguities in the coverage of transactions performed by notaries, lawyers and accountants should be removed. The requirements for enhanced monitoring of higher risk categories or transactions called for by the FATF Recommendations should be extended to the sector.

30. Although there is some level of awareness and effectiveness in within the sector, implementation generally needs to be strengthened, especially for TCSPs, and new or revised guidelines need to be issued. In addition to the shortcomings identified for the financial sector, heightened professional secrecy provisions for lawyers, notaries and accountants may be contributing to the low level of reporting of suspicious transactions.

31. The supervisory system is generally in place for the sector, but it mostly lacks resources and expertise. The sanctioning regime, which appears to be proportionate and dissuasive for the lawyers and notaries, needs to be developed for the other professions.

32. Measures to reduce the reliance on cash appear insufficient, considering the important quantity of large denomination banknotes issued by the OeNB.

### **Legal Persons and Arrangements and Nonprofit Organizations**

33. Austria mainly relies on a central registration of all types of legal persons, including foundations. However, access to relevant ownership information is hampered by several features of the system, notably limited requirements to register changes in ownership, the possibility for companies to issue bearer shares, and the option for private foundations to record beneficiaries' names in non-public appendixes to founding deeds.

34. The *Treuhand* is a very common feature of the Austrian economy. A partial registration system is in place which is limited to financial assets and is mandatory only for some of the trust service providers, i.e., lawyers and notaries. There are no measures to ensure the transparency of foreign trusts operated in Austria.

35. Obligations for NPOs to ascertain and maintain information about their ownership structure and transactions should be expanded.

### **National and International Cooperation**

36. Mechanisms for domestic cooperation and coordination are institutionalized and embedded into the Federal Constitution. Various policy and operational *fora* have been established under the lead of the Ministry of Finance where national competent authorities exchange information on AML/CFT issues and coordinate their respective activities.

37. Austria has enacted legislation that encompasses all key requirements of the international conventions regarding mutual legal assistance, signed several bilateral treaties with neighboring states, and shortened domestic procedures to improve the processing of information requests. The country may provide a range of measures of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings initiated by other countries. The legal regime which applies to foreign requests for confiscation is comprehensive. The extradition framework is not entirely in line with the FATF standard and its effectiveness was not established.

38. The provision of mutual legal assistance nevertheless suffers from some shortcomings. In particular, the strict requirements for lifting bank secrecy and the extensive scope of the legal privilege slow down the provision of mutual legal assistance.

39. Supervisory authorities have a fairly comprehensive regime for international cooperation on anti-money laundering. Weaknesses have been identified regarding international cooperation on combating terrorism financing, with the A-FIU not being legally empowered to exchange information, and concerning international cooperation by law enforcement authorities, which lacks effectiveness.

## 1. GENERAL

### 1.1 General Information on Austria

40. Situated in the heart of central Europe, Austria is an alpine country with a land area of almost 84,000 square kilometers and a population of just over 8 million inhabitants. Austria, along with all its neighboring countries, Germany, the Czech Republic, Slovakia, Hungary, Slovenia, and Italy, are Member States of the European Union (EU), with the exception of Switzerland and Liechtenstein<sup>1</sup> on its western border. German is the official language, while Croatian, Hungarian and Slovenian have the status of local official languages in some parts of the country.

#### *Economy*

41. Austria is a well developed and competitive market economy, which benefits from a successful integration to the global economy, and from the single EU market, which it joined in 1995. Its robust economic performance, which has repeatedly outgrown EU average growth, comes from a network of small and mid size industrial enterprises, and a growing service sector, supported by a highly skilled workforce. Intrinsic economic strengths are reinforced by social and political stability, based on a longstanding culture of cooperation among institutionalized interests groups and political parties (Social Partnership). Austria remains one of the wealthiest countries in the EU, with a GDP per inhabitant of EUR 31,139 (2006), well above the member country average of EUR 24,628.

42. As a member of the Euro zone, Austria is also attractive to foreign investors for its access to the EU market and its proximity to new European emerging economies. Geographical proximity, as well as strong cultural and historical ties, fostered the early development of activities in Central Eastern and Southeastern Europe (CESE) countries. Austrian banks, in particular, have acquired leading positions in these economies, which accounted for a significant share of their income in recent years.

#### *System of Government*

43. Austria is a democratic republic established as a federal state comprising nine autonomous states (*Länder*): Burgenland, Carinthia, Lower Austria, Salzburg, Styria, Tyrol, Upper Austria, Vorarlberg, and Austria's capital, Vienna. Initially enacted in 1920 and reintroduced in 1945, the Federal Constitution assigns specific legislative and executive powers to the federal state and to the *Länder*, with a larger share of prerogatives given to the federal level. The parliament consists of two chambers. Elected by direct popular vote to a six year mandate, the Federal President (*Bundespräsident*) is the head of state; he commands the army and represents the country abroad. He designates the Federal Chancellor (*Bundeskanzler*), usually the leader of the party with most seats in the National Assembly (*Nationalrat*), and appoints the vice Chancellor and the ministers; he convenes -and may dissolve- the *Nationalrat*. The *Bundeskanzler* leads the government and exercises all executive functions which are not assigned to the *Bundespräsident*. Most of the drafts for bills are

---

<sup>1</sup> Liechtenstein is a member of the European Economic Area.

formulated by the ministries, and must be approved unanimously by the government before being sent to parliament.

44. The legislative function consists mainly of the *Nationalrat*, jointly with the Federal Assembly (*Bundesrat*). The *Nationalrat* is designated by direct popular vote on a proportional representation basis for a five-year term, whereas the *Bundesrat*'s members are delegated by the assemblies of the *Länder*, in proportion to their population. In the legislative process, the *Bundesrat* has only a veto power which can be overruled by the *Nationalrat*. The parliamentary bodies are empowered to monitor the activities of the federal government, and to voice their wishes in the form of parliamentary resolutions on the implementation of executive powers. The constitution provides also mechanisms of direct democracy: voters can intervene directly in the political process by legislative initiatives and referendums. Constitutional laws, or provisions specified as constitutional in other laws, have to be passed by the *Nationalrat* by a two-thirds majority vote and a quorum of half of the members, and may be subject to a referendum if requested by one-third of the deputies.

45. In each of the *Länder*, the state government, elected by the state parliament (*Landtag*), and the governor act as the state executive branch. In matters relating to indirect federal administration, the state governor and the state authorities wield federal executive power and are subject to directives issued by the federal government and the federal ministers. Legislation passed by a *Landtag* is subject to the federal government's approval when its execution requires the cooperation of federal bodies.

#### ***Legal System and Hierarchy of Legal Source***

46. Austria is a civil law country. The Federal Constitution states that the federal state is the source of all legal jurisdictions, and guarantees the right of any individual person to proceedings before a lawful judge. Criminal law and civil law matters, except for real property, belong to the federal competence, as well as the administration of justice, and the organization and command of the federal police. Judges are independent in the exercise of their functions and can be dismissed or removed only by a judicial decision. They are appointed by the *Bundespräsident*. Criminal procedures are initiated on, and defined by, the claims of the public prosecution which is in charge of protecting the public interest of justice in penal affairs. The procedure, in which hearings are oral and public, follows the Code of Criminal Procedure (*Strafprozessordnung, StPO*). Offices of public prosecution are structured hierarchically and placed under the Federal Minister of Justice's authority.

47. Within the judicial system, a distinction is drawn between private law and public law jurisdictions. Private law jurisdictions, which are competent for all civil and criminal law matters, are organized in district courts (*Bezirksgerichte*) and regional courts (*Landesgerichte*). *Bezirksgerichte* (about 140) are competent as courts of first instance for lesser civil cases and offenses (value in dispute below EUR 10,000 and offenses subject to a fine or a sentence not exceeding one year of prison), and decisions are taken by a single judge. The 17 *Landesgerichte* act either in appeal of *Bezirksgerichte*'s decisions, or as first instance court in civil and criminal cases above *Bezirksgerichte*'s competence. For cases involving crimes subject to more than five-year imprisonment, the court is constituted by a jury of eight people, in addition to three professional judges. Four Courts of Appeal (*Oberlandesgerichte*) in the country decide in second instance on *Landesgerichte* cases. Each president of *Oberlandesgerichte* is responsible for the administration of justice in his region and reports directly to the Federal Minister of Justice for these matters. The Supreme Court (*Oberster Gerichtshof*), the highest judicial instance in Austria, hears all civil and

criminal cases at last instance. Its decisions are not legally binding, but, in practice, they provide direction as to lower courts decisions.

48. Independent administrative tribunals review the legality of decisions and exercise of power by the administrative authorities. The Administrative Supreme Court (*Verwaltungsgerichtshof*) seats in Vienna.

49. Administrative bodies can sanction administrative crimes and disciplinary matters under the administrative penal law. Appeals are brought to the Independent Administrative Chamber (*Unabhängiger Verwaltungssenat*) and to the Constitutional Court (*Verfassungsgerichtshof*). The *Verfassungsgerichtshof* pronounces also on the civil rights of the citizens, the conformity of laws with the constitution, claims on the federal state and *Länder*, or conflict of competence between jurisdictions.

### ***Transparency, Good Governance, Ethics, and Measures Against Corruption***

50. Austria, which ranks 12<sup>th</sup> out of 180 countries in the 2008 Transparency International Corruption Perception Index, figures regularly among the countries which are the less exposed to corruption. The criminal responsibility of legal entities and partnerships has been established, and both the payer and the recipient of a bribe face criminal penalties.

51. Austria is an active participant to international agreements and *fora* against corruption. It is party to the 2003 United Nations Convention against Corruption, which it ratified on January 11, 2006, and is involved in the voluntary pilot program aimed at designing methods for assessing the implementation of the Convention. Amendments to the Criminal Code (*Strafgesetzbuch, StGB*) were passed in 2008 in order to satisfy the requirements set out in the Convention, as regards to provisions on bribery of deputies.

52. Austria has signed the Council of Europe's criminal law and civil law conventions on corruption. The latter only has been ratified and came into force on December 1, 2006. In June 2008, the *Groupe d'États contre la Corruption* (GRECO) conducted an evaluation of the country's compliance with the Council of Europe anti-corruption standards which covered the themes of GRECO's First and Second Evaluation Rounds. The evaluation report concluded that "Austria is at an early stage in the area of the fight against corruption" and that a concerted approach to the issue is lacking.

53. Additionally, Austria has ratified the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, and is a member of the OECD Working Group on Bribery in International Business Transactions.

54. On the EU-level, Austria has signed, ratified and implemented the First Protocol to the Convention on the Protection of the Communities' Financial Interests and the Convention on the Fight against Corruption Involving Officials of the European Communities or Officials of Member States of the European Union. It has also ratified the Second Protocol to the Convention on the Protection of the Communities' Financial Interests.

## 1.2 General Situation of Money Laundering and Financing of Terrorism

### *Predicate Offenses*

55. Theft, drug trafficking and fraud are the main predicate crimes in Austria according to the statistics of convictions and investigations (see detailed statistics under section 2.1.1). Among other major proceed-generating offenses, the authorities identify human being trafficking, burglaries and smuggling. Austria is considered by EUROPOL as one of the four main destination countries for human being trafficking in the EU. The number of convictions for drug trafficking, theft, smuggling, corruption and bribery decreased sharply since 2004.

56. According to the authorities, in the case of theft and burglary, the proceeds are usually from predicate crimes committed in Austria. As regards narcotics, a part of the illicit proceeds were gained in Austria, while profits from fraud or smuggling are usually made abroad. The authorities did not provide any study on the revenue generated by the major sources of illegal proceeds or on the losses and damages resulting from criminal activities.

57. In comparison with other EU Member States, the crime level in Austria is among the lowest. In 2006, Austria was among the three countries of the 27 members of the EU that had the lowest number of homicides per inhabitant and around 29 cases of drug trafficking per 100,000 inhabitants were recorded, to compare with an average of 59 at the EU level.

### *Money Laundering*

58. According to the authorities, the most important money laundering problems faced by Austria are money remittance systems, offshore business and *hawala*. Money remittance systems are considered as the main tool used by drug-traffickers, internet-fraudsters, pickpockets, traffickers in human beings and burglars to launder money. Concerning offshore business, the authorities noted, as a recent trend, that companies are founded by “remote methods” and that individuals taking decisions (economic operators) often rent virtual office space with additional services, such as telephone and/or fax switching, in writing and for advance payments. The criminals attempt to create many different spheres of influence, for example by spreading their activities over various countries, using services (accounts, virtual office space, address services/post boxes, place of registration, etc.). Finally STRs and undercover investigations convinced the authorities that *hawalas* are mainly used by foreign criminal organization and networks.

59. The authorities did not conduct any study on the evolution of the pattern of money laundering following the introduction of AML measures or on the types of groups involved in laundering operations. They consider that Austria’s exposure to the risk of money laundering is low.

60. In 2007, the A-FIU received 1,085 STRs, rising from 373 cases in 2004. More than 95 percent of the declarations came from banks, including one single money remittance institution counting for a sizeable share. It has to be noted that information on phishing emails and 419 letters/emails are counted among the STRs. The number of ML convictions is very low. According to Statistics Austria, only three convictions for money laundering have been pronounced in 2005 and in 2006. The penalties provided for these convictions were extremely low, and the most severe penalty imposed was a one to three years imprisonment sentence pronounced in 2006. The authorities explained that the convictions are counted only in relation to convictions for the offense which has

the highest punishment (which is hardly the case for ML, when this is concurrent with other crimes). According to separate statistic compiled by the A-FIU and based on the actual number of ML charges underlying a conviction, there were 12 ML convictions in 2003, 10 in 2004, 5 in 2005, 10 in 2006 and 18 in 2007. The authorities further indicated that the low figures can be explained by the lack of criminalization of self-laundering in Austria and by the fact that the prosecutors prefer to indict the ML activities under “participation”, because a higher penalty provided in the case of participation in the predicate offense can be applied and, in practice, it is easier to prove participation in the predicate offense than the ML activity as a stand-alone crime.

61. In the absence of studies, the assessor team reviewed the Austrian and international press during a two year period before the assessment. A number of cases involving politically exposed persons from Eastern Europe, Central Asia, the Baltic States and the Balkans have been mentioned. The most common typology is that the predicate offense is committed abroad and the funds are allegedly laundered in Austria. The press reported a number of mutual legal assistance, extraditions requests and investigations in cases involving foreign PEPs. Financial investigations relating to corruption or embezzlement schemes by major foreign companies were also reported in the press. Finally, the press also mentioned several cases of suspicion of ML-related schemes involving subsidiaries of Austrian banks in CESE. This situation has led the Austrian parliament to consider the Austrian bank’s eastern businesses and their possible relation with ML in an inquiry concerning the Austrian banking supervision system and two commercial banks in 2007.

62. The absence of comprehensive risk analysis conducted by the authorities, associated with the general view in financial and non-financial institutions that the level of ML risk is low in Austria, may be a source of vulnerability in a country that attracts significant foreign financial flows based, among others, on a tradition of secrecy. It has to be noted that the aggregated balance sheets of banks show a growing trend in the ratio of foreign nonbank deposits to total nonbank deposits, amounting to 17 percent in 2007, after raising more than 20 percent from the 2005 level.

### ***Financing of Terrorism***

63. The authorities deem the risk of FT in Austria low, compared with other European jurisdictions. There have only been a few cases of terrorism investigations in the recent years. In 2007, eight persons were arrested for terrorist-related offenses, five of them related to Islamist organizations, and three related to right-wing organizations. On March 12, 2008, a court condemned a couple in Austria on charges of membership in a terrorist association (*Al-Qaeda*), threatening the Austrian Government and attempted coercion for producing an *Al-Qaeda* promoting video. The Supreme Court annulled the verdict on procedural issues and remitted it to the court for re-examination. It also needs to be noted that Austria hosts a number of minorities, including of Kurdish origin. In this context, members of an EU and US designated terrorist group were found to have stayed in Austria in 2007. The authorities assume that, like in several other EU member States, a very small part of the Kurdish community collects funds for terrorist purposes, but they currently have no available evidence to confirm this assumption. There is also no information on how FT techniques and trends have changed following the introduction of counter-terrorist financing measures.

64. In the last four years, the authorities consider that the suspicious cases and complaints did not only rise in quantity, but also in quality. While there have been fewer matches with the different terrorist lists, more STRs have been registered due to the increased due-diligence by reporting

entities. The authorities mentioned two cases that they consider illustrating the range within terrorist financing. In the first case, legally acquired money was transferred via official bank transfers to organizations in the Near East, whereas in the second case, the amounts acquired by traditional criminal activities were transferred as quickly and anonymously as possible via “Money Transmitter Systems.” Both cases were initiated by STRs from the financial sector.

65. Concerning the transfer methods, the authorities assume that new payment methods—such as Internet-based transfer systems or transfer by use of mobile phones—will gain in importance, since these methods result in advantages for the terrorist organizations such as few and weak control possibilities and faster transfer. To date, however, such methods have not been ascertained in Austria yet and no such cases of suspicion have come to the authorities’ knowledge.

66. Between 2003 and 2006, 18 criminal cases related to FT have been registered, but none of them have led to an indictment. In 16 cases, the proceedings were dismissed by the public prosecutors. Two FT cases initiated in 2006 are still pending. In 2007, four new FT cases were registered, thereof two criminal investigations by public prosecutors, and two preliminary investigations by investigative judges; three of them have been terminated, one case is still pending. Therefore there are actually three FT cases pending, none of them has resulted in an indictment. Until 2007, there have been no convictions of FT.

### **1.3 Overview of the Financial Sector and DNFBP**

#### ***Overview of the Financial Sector***

67. Austria has a developed and diversified financial sector, which contribution to the country’s total value added was 5.4 percent in 2005.<sup>2</sup> The core of the country’s financial system is formed by the credit and domestic financial institutions, dominated by a few large groups which conduct a full range of financial activities, notably through insurance and mutual fund management subsidiaries. The five largest credit institutions hold almost 50 percent of total banking assets, and two of them are foreign-owned. Post office’s financial services have been privatized. There are 12 exchange offices in the country, mostly located in Vienna. All these activities are conducted by credit institutions and regulated by the Banking Act (*Bankwesengesetz, BWG*).

68. Thirty-one out of the 82 insurance companies which are active in Austria are engaged in the life business. There are no independent reinsurance companies. The insurance sector remains small in comparison with other EU countries (total assets equal 32 percent of GDP, vs. 63 percent in the EU), notably in the life segment, which is not supported by incentives granted by some other tax regimes. The major insurance companies are associated with Austrian banking groups. Insurance activities fall under the provisions of the Insurance Supervision Act (*Versicherungsaufsichtgesetz, VAG*).

69. Insurance products are also marketed by insurance intermediaries. These independent agents and brokers are natural or legal persons who can work on preparing for the conclusion of contracts, or conclude contracts, as well as participate in the administration and performance of such contracts.

---

<sup>2</sup> Austria ranks in the second tier of OECD Member States for value added by finance and insurance activities (source: OECD in Figures 2008 [www.oecd.org/infigures](http://www.oecd.org/infigures)).

There are 18,374 registered intermediaries who are regulated by the Trade Act 1994 (*Gewerbeordnung, GewO*).

70. The securities business includes:

- 145 investment firms (*Wertpapierunternehmen*) which can perform the following functions: reception, transmission, execution of orders, portfolio management on mandate, investment advice and underwriting; and 163 investment service providers/undertakings (*Wertpapierdienstleistungsunternehmen*) which can receive and transmit orders in transferable securities and units in collective investment undertakings (only to investment firms). Both are regulated by the Securities Supervision Act (*Wertpapieraufsichtsgesetz, WAG*);
- 29 investment fund management companies which are credit institutions, regulated by the BWG. The three major management companies account for 57 percent of the whole business; and
- 2,364 domestic investment funds which manage EUR 166 billions of assets. Total assets under management, which doubled since 2000, amount to 64 percent of the GDP, well above the EU average, 57 percent (2006). Many of the investment funds are promoted and managed by banks. They do not enjoy legal personality, and their assets are deposited with banks. The number of foreign investment funds marketed in Austria has also grown substantially over the recent years (4,962 in 2007).

71. Other segments of the capital market include the debt securities which volumes are comparable to those in similar EU countries, and the stock market, which total capitalization is small in comparison to EU peer countries. Securities clearing is processed by CCP-A. The *Oesterreichische Kontrollbank (OeKB)* operates securities trading settlements and is the Central Securities Depository for Austrian issuances; as a credit institution, it is subject to the AML/CFT provisions of the BWG. The Stock Exchange Law (*Börsegesetz, BörseG*), regulates the stock and commodity exchange activities.

Statistical Table 1. Categories of Financial Institutions  
(As of end-December 2007)

	<b>Number</b>	<b>Assets (EUR billion)</b>
Credit Institutions	871	899
Domestic Financial Institutions	(952-13,459)	Na <sup>3</sup>
Non-Life Insurance Undertakings	51	23 <sup>4</sup>
Life Insurance Undertakings	31	60
Pensions Funds	20	13
Investment Firms	145	-
Investment Service Providers	163	-
Domestic Investment Funds	2,364	164
Foreign Investment Funds	4,962	na

(Source: FMA)

72. Organic growth being limited in the competitive domestic market, Austrian banks and insurance companies have greatly developed their cross border business in recent years. They have become key players in most of the financial markets in CESE and more recently in some CIS countries. Banks have expanded their activities in the retail and corporate banking business, and insurance companies collected 24 percent of their premium written in CESE countries in 2006.

Statistical Table 2. Market shares of Austrian banks in CESE and CIS countries

<b>Countries</b>	<b>Share of total banking assets (as of December 2007)</b>
Bosnia and Herzegovina, Croatia, Slovak Republic, Albania, Serbia, Czech Republic	≥ 35%
Hungary, Bulgaria, Romania, Slovenia	15-35%
Ukraine, Poland, Belarus, Russia	≤ 15%

(Source: FMA)

73. Additionally, many Austrian banks market to both nonresident and resident foreign customers, promoting the country's reputation for political stability and strict banking secrecy provisions, as well as its attractive tax regime for foreign investors. About 30 credit institutions offer private banking and wealth management services in Austria. No data are available for total assets under management in the private banking business segment, but aggregated balance sheets of banks show a growing trend in the ratio of foreign nonbank deposits to total nonbank deposits, which was 17 percent in 2007 compared to 14 percent in 2005.

<sup>3</sup> Not available.

<sup>4</sup> As of December 31, 2006.

74. Notably, because of the dominant cooperative structure, Austria has a large number of banks. The three main cooperative banks, which generally target different segments of the market, are organized on a decentralized tiered structure with apex entities providing limited centralized services in the areas of payment and settlement, liquidity management and funding.

Statistical Table 3. Credit institutions (December 31, 2007)

	Number	Assets(EUR b)
Joint Stock and Private Banks <sup>5</sup>	51	251
Savings Banks ( <i>Sparkassen</i> )	56	150
Rural Credit Cooperatives ( <i>Raiffeisenbanken</i> )	558	222
Industrial Credit Cooperatives ( <i>Volksbanken</i> )	70	69
Mortgage Banks ( <i>Landeshypothekenbanken</i> )	11	88
Building Societies ( <i>Bausparkassen</i> )	4	21
Special banks ( <i>Sonderbanken</i> )	96	87
<i>Of which:</i>		
<i>Investment Fund Management Companies</i>	29	166 <sup>6</sup>
<i>Exchange Offices</i>	12	Na
EEA Branch offices	25	11
<b>Total</b>	<b>871</b>	<b>899</b>
<i>Credit Institutions from EEA Member states<sup>7</sup></i>	392	

(Source: FMA)

75. Most of the institutions operate as universal banks. The major banks maintain an extended network of domestic and international subsidiaries and branches, and the global domestic distribution channel is large by European standards (each branch serves on average 1,945 people, for an EU average of 2,569).

76. Domestic financial institutions, as defined in Article 1, paragraph 2 of the BWG, are authorized to conduct at least one of the following activities as their main activity: leasing, advice on capital structure, industrial strategy, mergers and acquisitions, credit reporting services, and safe deposit services.

Statistical Table 4. Domestic Financial Institutions

<sup>5</sup> In the FMA nomenclature, private banks are commercial banks.

<sup>6</sup> Assets under management.

<sup>7</sup> Foreign financial institutions licensed in their home state and authorized to operate in Austria by virtue of cross-border provision of services under the Single European Market which applies to EU and EEA Member States.

Activities	Number of Institutions
Leasing	950
Safe deposit services	2
Advice (management consultants) <sup>8</sup>	12,507

77. All traditional and new payment methods are used in Austria. Supported by a dense network of point of sale (POS) terminals, debit cards (6.9 million cards in 2005) are more common than credit cards (1.1 million cards) for which the number of transactions remains relatively small, but the average payment is relatively high. The use of other electronic payments, such as prepaid cards, is increasing, but remains limited; and cash, which is notably distributed through a large number of ATMs, is still widely used for day-to-day payments.<sup>9</sup> Banks offer internet banking services which are limited to transactions on, and consultations of, existing accounts.

78. The BWG defines a large array of banking activities, the provision of which is restricted to credit and domestic financial institutions according to its Article 1, paragraph 2. Under the BWG, are defined as banking transactions all types of lending and deposit business and securities trading and underwriting, as well as the management of investment funds, and foreign exchange and remittances operations. Credit institutions are institutions authorized to carry out one or more banking transactions defined in the law, while domestic financial institutions (according to Article 1, paragraph 2 BWG) have limited allowed activities (leasing, financial advice, and safe deposits notably).

79. The following table sets out the types of Austrian financial institutions that can engage in the financial activities that are within the definition of financial institutions in the FATF Recommendations.

Statistical Table 5. Financial Activities Listed in the Glossary of the 40 Recommendations which are Conducted by Financial Institutions in Austria

Financial Activity	Type of Financial Institution	AML/CFT	
		Legislation	Supervision
1. Acceptance of deposits and other repayable funds from the public (including private banking)	Credit Institutions	BWG	FMA
2. Lending (including consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting))	Credit Institutions	BWG	FMA
3. Financial leasing (other than financial leasing arrangements in relation to consumer products)	Credit Institutions	BWG	FMA
	Domestic Financial	BWG/AVG	Local District

<sup>8</sup> No data available which differentiate management consultants (*Unternehmensberater*) who operate as DNFBPs, from those carrying out only the activities defined in Article 1 paragraph 2 of the BWG.

<sup>9</sup> Source: *Payments and Securities Settlements Systems in the EU*, ECB August 2007.

	Institutions		Authorities
4. The transfer of money or value (including financial activity in both the formal or informal sector, but not including any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds)	Credit Institutions	BWG	FMA
5. Issuing and managing means of payment (e.g., credit and debit cards, cheques, traveler's cheques, money orders and bankers' drafts, electronic money)	Credit Institutions	BWG	FMA
6. Financial guarantees and commitments	Credit Institutions	BWG	FMA
7. Trading in money market instruments, foreign exchange; exchange, interest rate and index instruments; transferable securities; and commodity futures trading	Credit Institutions	BWG	FMA
8. Participation in securities issues and the provision of financial services related to such issues	Credit Institutions	BWG	FMA
9. Individual and collective portfolio management	Credit Institutions	BWG	FMA
	- Investment Firms - Investment Fund & Real Estate Investment Fund Mngt Cies	WAG	FMA
10. Safekeeping and administration of cash or liquid securities on behalf of other persons	Credit Institutions	BWG	FMA
11. Otherwise investing, administering or managing funds or money on behalf of other persons	Credit Institutions	BWG	FMA
	- Investment Firms - Investment Fund & Real Estate Investment Fund Mngt Cies	WAG	FMA
12. Underwriting and placement of life insurance and other investment related insurance (including insurance undertakings and to insurance intermediaries (agents and brokers))	Life Insurance Undertakings	VAG	FMA
	Insurance Intermediaries	GewO	Local District Authorities
13. Money and currency changing	Credit Institutions	BWG	FMA

80. The Financial Market Authority (FMA) is the integrated regulator and supervisor for the financial sector, with the exception of domestic financial institutions and insurance intermediaries which are supervised by the local district authorities. As a result of a recent revamp of the supervision framework (January 2008), the Austrian National Bank (*Oesterreichische Nationalbank, OeNB*) has sole responsibility for conducting offsite monitoring and onsite examinations of banks, but the overall responsibility for banks' regulation and enforcement stays with the FMA. The focus of OeNB

supervision is on systemic banks, and external auditors retain the function of assessing compliance with regulations of all credit institutions annually.

## Overview of the DNFBP Sector

### *Casinos*

81. Organization of games of chance is regulated in the Gambling Law (*Glücksspielgesetz, GSpG*). The GSpG does not know the words “casinos” and “internet casinos”, but refers to gaming houses (*Spielbanken* defined in Article 21, paragraph 1 GSpG) and electronic lotteries (*Elektronische Lotterien*, defined in Article 12a GSpG) which may be run as internet casinos, offering casino games with non-face-to-face transactions between the customer and the licensee.

82. The gaming legislation establishes a monopoly of the Federal Government executed by a system of licenses granted by the Federal Ministry of Finance (MoF). Currently all legally permitted licenses have been assigned to only two licensees, *Casinos Austria AG* (CASAG) for 12 Austrian casino licenses and the *Österreichische Lotterien GmbH* (ÖLG) for electronic lotteries. There are currently legal proceedings regarding card casinos, which have developed quickly in recent years and are not regulated, but that the authorities consider as game of chance providers.

83. The MoF is the supervisory authority for casinos and internet casinos with extensive supervisory powers. The following table gives an overview of casinos and internet casinos currently operating in Austria:

Statistical Table 6. Activity of Casinos in Austria

Type	Number	Gaming Revenue (2007, EUR m.)	Betting Volume (2007, EUR m.)	Licensing and Supervisory Authority (incl AML/CFT)	
Casinos	12	194	4.215	MoF	MoF
Internet Casinos	1	35	-	MoF	MoF

84. The total betting volume more than doubled between 2005 and 2007 and foreigners account for 70 percent of the bets.

### *Real Estate Agents, Dealers in Precious Stones and Metals, TCSPs*

85. All these professions are regulated by the GewO and have to be registered. The competent authority for authorization and registration, prudential or market conduct supervision, and for AML/CFT supervision are the local district authorities (*Bezirksverwaltungsbehörden*), in cooperation with the police. Local district authorities are under the command of the States' Governors who are directly under the control of the Federal Ministry of Economy, Family and Youth (MoE) as the supreme authority (police authorities are under the control of the Federal Ministry of the Interior, MoI).

86. Real estate agents are involved in transactions for their clients concerning the buying or selling of real estate. They are allowed to represent their clients in front of authorities. As shown in the table below, their number has increased in recent years:

Statistical Table 7. Real Estate Activity in Austria

	2006	2007	2008
Number of Real estate Agents (including real Estate Management, Building Contractors)	8.514	8.734	8.954
Number of Branches	1.683	2.151	671

87. In Austria, all dealers—not only the ones dealing with precious stones and metals—fall under the AML/CFT legislation when carrying cash transactions above EUR 15,000. No information was available on the precise number of dealers in precious stones and metals.

88. According to the authorities, the profession of management consultant (*Unternehmensberater*) carries out the functions of TCSPs regarding the FATF definition, and has to comply with the AML/CFT provisions of the GewO. But their core function is to give advice to companies, not to provide the services listed in the FATF glossary concerning TCSPs. In 2008, 12,507 management consultants were registered with the Austrian Federal Economic Chamber (*Wirtschaftskammer Österreich, WKO*).

89. Other professions used to provide services which are listed in the FATF definition of TCSPs. These are office services, consisting of writing, messenger services, receipt and forwarding of messages (*Büroarbeiten bestehend of Schreibearbeiten, Botengängen, Entgegennahme und Weiterleitung von Nachrichten*) and office services consisting on provision of office equipment and office facilities (*Büroservice zurverfügungstellen von Büroeinrichtungen*). Six hundred and seventy-nine firms are registered with the WKO in these two categories. Pursuant to the new provisions of the GewO, each provider of an activity listed by the FATF as TCSP will have to be registered as a management consultant. The implementation of these provisions was not effective at the time of the on-site visit.

### ***Accountants***

90. The two professions of chartered public accountants-tax consultants (*Wirtschaftstreuhänder*), and certified management accountants-accountancy professions (*Bilanzbuchhalter*) perform activities that are listed in FATF Recommendations 12 and 16. Both professions are authorized to prepare for or carry out transactions for creating, operating or managing legal persons or arrangements, and buying and selling business entities. They also can assist in managing client money, securities, or other assets.

91. In March 2008, 8,027 natural persons and 2,345 companies were registered with the Chamber of Chartered Accountants and Tax Consultants, and 2,079 natural persons and 62 companies were registered for the Accountancy Profession (2,052 certified management accountants, 61 certified management accountant companies, 3 bookkeepers, 24 payroll accountants and 1 payroll accountant-company).

### **Lawyers**

92. Lawyers typically engage in the representation of parties before all courts and authorities in Austria and the representation and advice of parties in all court and out-of-court, in all public and private matters. They are organized to the Lawyer's Act (*Rechtsanwaltsordnung, RAO*). They are also able to engage in the following activities:

- the purchase or the sale of real estate or enterprises;
- the administration of money, securities or other assets, the opening or administration of bank accounts, saving accounts or accounts regarding securities; and
- the foundation, operation or administration of trust companies, companies or similar structures like endowments or foundations, including the procurement of means necessary for the foundation, operation or administration of companies.

93. The number of lawyers increases every year. There were 4,494 lawyers registered in the list of Austrian lawyers and 47 lawyers registered in the list of established European lawyers in 2003, but 5,129 Austrian lawyers and 81 European lawyers in 2007. The competent authority for supervision of the profession, including AML/CFT supervision, is the Board of the Bar Association (*Ausschuss der Rechtsanwaltskammer*).

### **Notaries**

94. Following the legal tradition of continental Europe, Austrian notaries are Latin (civil law) notaries. Organized through the Notaries' Act (NO), they are self-employed law experts who provide advice to their clients and set up agreements and authentic acts as instructed. As court commissioners, they are also vested with quasi-judicial functions. Notaries are appointed by the government, and endowed with carrying out public functions. They are not public servants, however, and bear the economic risk of running their business.

95. The statutory scope of action of Austrian civil law notaries includes the following activities listed in FATF Recommendations 12 and 16:

- the purchase or the sale of real estate or enterprises;
- the administration of money, securities or other assets, the opening or administration of bank accounts, saving accounts or securities accounts; and
- the foundation, operation or administration of trust companies, companies or similar structures like endowments or foundations, including the procurement of means necessary for the foundation, operation or administration of companies.

96. Notaries play an important role as trustees, and must be capable of exercising accepted trusts independently (*Treuhandenschaft* not in the meaning of an "Anglo-American trust"). Notaries must record trusts in the Trust Register of Austrian Notaries set up by the Austrian Chamber of Civil Law Notaries before making any disposition of the trust property, in order to ensure maximum security and to allow for monitoring of compliance with the duties arising under the execution of trusts.

97. Austrian civil law notaries carry the official title of a notary public. The MoJ is authorized to set up new notarial offices, to close existing ones or to transfer a notarial office to another place by

way of official ordinance. Currently, there are 478 notaries and 381 notarial candidates in Austria. Notaries are tied to the bounds of their notarial offices. The competent regional Chamber of Civil Law Notaries exercises professional supervision of notaries in respect of the exercise of their official duties and professional conduct.

#### **1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements**

98. The Austrian Law recognizes the following types of legal persons:

- Limited liability company (*Gesellschaft mit beschränkter Haftung*);
- Joint-stock company (*Aktiengesellschaft*);
- European Society (*Europäische Gesellschaft*);
- Cooperative society (*Erwerbs- und Wirtschaftsgenossenschaft*);
- European cooperative (*Europäische Genossenschaft*);
- Association (*Verein*); and
- Private foundation (*Privatstiftung*).

99. Legal persons come into legal existence by registration in the Commercial Register, which is maintained at the court of first instance on commercial matters (*Firmenbuchgericht*). The Commercial Register is accessible online to everybody via special websites authorized by the MoJ and against a small fee. There are local offices of the Commercial Register in each of the 99 districts in which Austria is divided.

100. Newly formed corporations must record the articles of incorporation and submit the application signed by all founders, members of the supervisory board and the board of management to the court responsible for the Commercial Register. When the court decides that all statutory requirements have been complied with, it will order the registration and publication in the official gazette (*Amtsblatt zur Wiener Zeitung*) and through the Internet (*Ediktsdatei*, available via [www.edikte.justiz.gv.at](http://www.edikte.justiz.gv.at)).

101. Associations have to be registered with the relevant local district authority or Federal Police Directorate (*Vereinsbehörde*), which can refuse the registration if the association, its purpose etc. infringe Austrian law. Each association is registered under a register number and listed in the Central Register of Associations (*Zentrales Vereinsregister, ZVR*). The *ZVR* is a public register, kept by the MoI and accessible online by anyone (<http://zvr.bmi.gv.at/Start>).

102. Foreign corporations can establish branch offices in Austria, which, before starting business, must be entered in the Commercial Register at the commercial court competent for the district where the branch has its seat. In this case, the disclosure requirements set forth in the case of companies incorporated under Austrian law will be applied analogically, based on the type of mother-company in the incorporating jurisdiction.

## 1.5 Overview of the Strategy to Prevent Money Laundering and Financing of Terrorism

### *AML/CFT Strategies and Priorities*

103. Austria has not formalized a specific AML/CFT strategy. As a highly developed, open and globally integrated country, Austria's international approach to combat money laundering and the financing of terrorism emphasizes multilateral coordinated action and cooperation, and the Austrian government actively supports the ongoing work in the EU, the UN, the Council of Europe, the FATF and other international *fora*. Priority is also given to the appropriate and timely implementation of the Directive 2005/60/EC of the European Parliament and of the Council of October 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Third EU ML Directive).

104. The MoF leads Austria's delegation to the FATF, and plays a major role in initiating and ensuring a timely transposition of European norms into the domestic regime. In application of the constitutional principle of cooperation between administrative authorities, defined by Article 22 of the Federal Constitutional Law (*Bundes-Verfassungsgesetz, B-VG*), several coordinating *fora* have been established at both executive and operational levels.

105. At the policy level, the quarterly Financial Market Committee (FMC) consists of the Director General responsible for Financial Market issues in the MoF (Chair), and the CEOs of the OeNB and the FMA; its ambit covers all financial market stability matters, including AML/CFT issues, and its recommendations have strong policy effect on the ministers and the parliament. In the monthly MoF/FMA *Jour Fixe* meetings, the FMA CEOs and MoF Deputy Director General responsible for financial market issues discuss further actions related to the FMC matters.

106. At the operational level, the focus is on developing and implementing policy measures: FATF coordinating meetings involve all authorities responsible for AML/CFT policy, supervision and enforcement (MoF, MoJ, FIU, BVT, MoFA, FMA, OeNB, MoE); in the AML/CFT Task Force, the MoF, FMA, BVT, A-FIU, OeNB and MoJ meet quarterly to assess new ML/FT trends and typologies, discuss operational problems, and review issues arising from the private sector; and the MoF and FMA AML/CFT *Jour Fixe* takes place monthly, and address operational issues relating implementation of the AML/CFT measures.

107. Austria has a long-standing practice of close and regular cooperation between the authorities and various institutionalized interest groups, represented notably by economic and professional groupings with compulsory membership. The department Bank and Insurance of the WKO published the first professional regulation for AML in 1989, and the WKO still makes a major contribution toward raising awareness of ML/FT risks among its members, especially the DNFBPs. In particular, a two-year activity plan is currently being drawn with the authorities to provide information on ML/FT trends and AML/CFT legislations to the private sector across the country.

108. Political commitment to combating ML and FT is also demonstrated through Austria's membership of, and participation in, many international *fora* which contribute to the global preventive efforts, notably UN and OECD Conventions on Bribery, Corruption, Drug and Organized Crime. Austria contributes to, and takes part in, UNODC activities, EU's specialized institutions (EUROPOL, EUROJUST) and EU's AML committees and task forces, as well as EU partnership

programs to develop legal systems, build institutional capacities and implement preventing measures to combat crimes, particularly ML/FT.

### ***The Institutional Framework for Combating Money Laundering and the Financing of Terrorism***

#### **Ministries**

##### *Federal Ministry of Finance (MoF)*

109. The MoF has a prominent role in the coordination of Austrian AML/CFT policy. It also submits proposals of amendments to legal acts concerning the regulation and supervision of the financial sector. The Tax and Customs Department is a unit within the MoF which has competency to propose revisions of the Customs Law and the Fiscal Penal Code, as regards to sanctions for any breach of the Custom Law. The MoF is the competent authority for proposing amendments to the GSpG for the licensing and supervision of casinos and internet casinos, including appointing state commissioners to the licensees.

##### *Federal Ministry of Justice (MoJ)*

110. The MoJ carries out an overall responsibility for criminal law, for example the StGB and the StPO. It is responsible for regulating the activities of lawyers and notaries, as regards to the Lawyer's Act, the Disciplinary Statute for lawyers and lawyer-candidates, and the Notarial Code. The MoJ has charge of international cooperation, especially extradition and Mutual Legal Assistance (MLA), including the transfer of proceedings to a foreign country. Additionally, it has a statutory role in legal acts relating to legal persons and arrangements.

##### *Federal Ministry of the Interior (MoI)*

111. Public security, criminal investigations, and law enforcement are the core functions of the MoI. Within the ministry, the Austrian Financial Investigation Unit (A-FIU) and the Federal Agency for State Protection and Counter-Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, BVT*) are the police and intelligence units specialized in combating ML and FT. The Associations Act and the supervision of its implementation fall also within its ambit.

##### *Federal Ministry for European and International Affairs (MoFA)*

112. The MoFA's functions cover matters relating to public international law, whether Austria's compliance with international obligations and the negotiation of international treaties, or the coordination of the country's policy for justice and home affairs in international and European *fora*.

##### *Federal Ministry of Economy, Family and Youth (MoE)*

113. In the area of AML/CFT, the MoE is responsible for preparing legislative proposals related to auditors, external accountants and tax advisors, trust or company service providers, real estate agents and dealers, including auctioneers, and insurance intermediaries. It has competency to issue related secondary regulations and guidelines, and, with its local district authorities, is the supreme authority for the supervision of the above-mentioned professions.

#### **Criminal Justice and Operational Agencies**

*The Austrian Financial Investigation Unit (A-FIU)*

114. The A-FIU is a police unit within the Criminal Intelligence Service (*Bundeskriminalamt, BKA*). It receives and investigates STRs, or mandate investigations to the national police services, but the BVT is solely competent to investigate FT related cases.

*Federal Agency for State Protection and Counter-Terrorism (BVT)*

115. Within the Public Security Department of the MoI, the BVT is competent for state protection, notably counter-terrorism and counter-terrorism financing, and is seconded by States' Agencies for Protection and Counter-Terrorism (*Landesämter für Verfassungsschutz, LVT*) in the nine *Länder*. BVT investigations can be initiated on the basis of information received from the private sector (Suspicious Transaction Reports, STRs, forwarded by the A-FIU), other national or foreign security authorities, or internal sources.

*Courts and Prosecution Authorities*

116. The Code of Criminal Procedure (StPO) provides for four different types of courts, depending on the maximum length of the possible sentence. Court rulings in civil law and penal law matters are the exclusive responsibility of independent judges. Judges are appointed by the MoJ on the basis of an objective selection procedure. The appointment of senior judges is reserved to the *Bundespräsident*.

117. The function of the public prosecution is to protect public interest in the administration of justice. This primarily involves conducting investigations, in cooperation with the criminal police, laying charges against persons, and representing the indictment in penal proceedings. Public prosecution offices are separate from the courts, and are bound by instructions received from the senior public prosecution offices and ultimately of the MoJ. The General Procurator's Office, set up with the Supreme Court, is directly responsible to the Federal Minister of Justice and does not have the right to issue any instruction to the offices of public prosecution and the offices of senior public prosecutors.

**Financial Sector Bodies**

*Financial Market Authority (FMA)*

118. The FMA serves as the integrated supervisor of all financial institutions<sup>10</sup> and activities, that is, banking, insurance, securities and pension fund activities. It is an autonomous institution under public law which is placed under direct parliamentary control. The FMA functions include issuing regulations, granting licenses, as well as supervising and enforcing prudential and AML/CFT requirements. Within the FMA, an AML Competence Center monitors international and domestic developments on AML/CFT issues and provides technical support to functional departments. The FMA is responsible for conducting specific AML/CFT examinations in financial activities which are in its remit.

*Central Bank (Oesterreichische Nationalbank, OeNB)*

---

<sup>10</sup> With the exception of domestic financial institutions (see below).

119. In 2007, the banking supervision functions have been restructured, the OeNB being granted sole responsibility for carrying out offsite analysis and conducting onsite examinations of credit institutions, while the FMA remains entrusted with regulatory, licensing and enforcement powers. Procedures and operational arrangements have been institutionalized to maintain close cooperation and regular consultation between the two institutions. The OeNB is, within the scope of the Foreign Exchange Act (*Devisengesetz, DevG*), also in charge of enforcing financial sanctions in international payment transactions.

## **DNFBPs**

### *Casino Supervisory Body*

120. The MoF is the responsible supervisory authority for casinos. The surveillance of casinos is conducted by a team of independent inspectors of the MoF. An appointed state commissioner attends all meetings of the supervisory board and the general meeting of the shareholders. Additionally, a special department of the Local Tax Authority for Fees and Transaction Taxes mandates independent inspections of casinos, in order to control proper determination of the tax base, such control contributing to the overall prevention of ML/FT. Local tax authorities report to the MoF.

### *Traders, TCSPs*

121. Under the responsibility of the MoE and the state governors, local district authorities are responsible for the licensing and prudential supervision of all activities conducted under the GewO, including trust or company service providers, real estate agents and dealers including auctioneers and insurance intermediaries. Their function includes checking compliance with AML/CFT measures and issuing administrative sanctions for regulatory breaches. The MoE can give instructions to lower level authorities. Since the last amendment of the GewO in 2008, police services must cooperate with and support the trade authorities in the execution of AML/CFT provisions.

### *Lawyers, Notaries and Accountants*

122. The Board of the Bar Association, where a lawyer is registered, is the responsible authority for monitoring compliance with professional regulations, including AML/CFT requirements. Board members are elected by the plenary meeting for a three-year term. Disciplinary offenses are to be handled by the Disciplinary Council, elected by the Bar Association.

123. The competent regional Chamber of Civil Law Notaries is the responsible supervisory authority for notaries, and this function includes verifying whether notaries comply with the provisions serving to prevent or fight ML or FT.

124. The Chamber of Chartered Public Accountants and Tax Consultants and the Parity Commission for the Accountancy Professions, which are the competent supervisory authorities for AML/CFT preventive measures for accountants, are subordinated to the MoE.

### *Registry for Companies and Other Legal Persons, and for Legal Arrangements*

125. The Central Register of Associations (ZVR) is administered by the MoI. The Commercial Register contains records about the ownership and control details for all companies and other legal

persons, and is administered by the Commercial Courts. Changes in ownership and control information must be kept up to date. All information is available to the public.

#### *Non-Profit Organizations (NPOs)*

126. NPOs are mainly organized as associations which are listed in a public register administered by the MoI. The MoI is the authority responsible for regulating associations and has the competence to give instructions to the lower level authorities. Associations (as well as other NPOs) with charitable or welfare purposes or purposes connected to a state-approved church are tax-exempted, independently of their legal form (association or otherwise). Tax authorities have to verify the purpose of the organization, based on the statutes and accounts. In 2002, the eight most important umbrella organizations (representing more than 350 charities and all catholic orders in Austria) signed a contract with the Chamber of Chartered Public Accountants and Tax Consultants on a seal of quality for donation organizations.

#### **Other Bodies**

127. The local district authorities, in the first instance, and the regional governors, as the second instance, are competent for the supervision of domestic financial institutions, according to the provisions of the General Administrative Procedure Act (*Allgemeines Verwaltungsverfahrensgesetz, AVG*).

128. The Austrian Federal Economic Chamber (*WKO*) and its nine state chambers, as well as other chambers of various professions (e.g., lawyers and notaries, accountants and tax consultants), play an important role in Austrian public life. Their duties include representation of membership interests domestically and internationally, as well as information and advisory service to their members. By law, governments are obliged to consult with the chambers on legislative projects and important regulations. Many legal provisions involve the chambers in decision-making and administrative procedures, and may entrust them with supervisory or regulatory powers.

129. In the course of their auditing work, external auditors carry out particular investigations on financial institutions' compliance with prudential and AML/CFT legal requirements and report on these issues to the FMA.

#### **Approach Concerning Risk**

130. Austria has transposed the Third EU ML Directive, including the risk-sensitive measures that it requires, into the Austrian legal framework, with effect on January 1, 2008. The authorities underlined that, as a member state, Austria contributed to the risk assessment and analysis conducted at the EU level and to the resulting legal provisions. The risk-based approach in place since January 2008 therefore, stems from the EU Directive; it is not the result of a domestic assessment of the overall money laundering and terrorist financing risk in Austria. The authorities pointed that some risk analysis had been conducted prior to the implementation of the EU Directive and resulted in the introduction of legal provisions such as those that require customers to indicate if they are acting on behalf of a third party, as well as those that subject non-face-to-face business to enhanced due diligence and include the money remittance business into financial activities subject to licensing. While this would indeed tend to indicate that some partial risk analysis was conducted at the time, it does not however point to a comprehensive assessment of the money laundering and terrorist

financing risks in Austria. It is unclear for instance why the level of risk posed by other areas of relevance to the Austrian financial sector (such as private banking for example) has not been assessed.

131. The new regime entrusts persons and entities subject to AML/CFT provisions with defining and operating preventive measures adjusted to risks, while it lists situations allowing lower or higher CDD. Persons and entities subject to AML/CFT provisions are required to conduct a risk-analysis of their business, using suitable criteria, and to take appropriate risk-based measures to ascertain customer information and conduct ongoing monitoring.

132. Austria's financial sector structuring in decentralized and multi-tiered groups results in a large number of financial institutions. Supervisors have long adopted a risk-sensitive approach to onsite examinations. Mission planning and inspection scope are based on assessments of ML and FT risks across institutions, and weaknesses in preventive measures detected by external auditors or OeNB and FMA supervisors.

### **Progress Since the Last Evaluation**

133. The last assessment of Austria compliance with the previous FATF Recommendations was conducted by the IMF in the course of the 2003 FSAP, using the former methodology. The assessors concluded that the overall legal and institutional framework was comprehensive and that Austria had achieved a good level of compliance with the FATF 40+8 Recommendations. However, they identified several areas which needed further strengthening:

- greater clarity in some of legal provisions, defining suspicion of money laundering and the obligation to screen unusual transactions;
- further guidance to financial institutions on AML/CFT duties, in particular on the identification of customers;
- enhanced monitoring of compliance by the supervisors in all financial institutions subject to AML/CFT obligations, including through on-site inspections; and
- sustained supervisory attention during the process of phasing out anonymous savings deposit accounts.

134. Subsequent legislative and regulatory revisions and the implementation of the Third EU ML Directive resulted in a large overhaul of the AML/CFT regime, addressing the above-mentioned concerns:

- identification and verification requirements, notably for beneficial owners in legal entities, and beneficiaries of insurance policies, have been strengthened, and implementing guidelines have been issued;
- a risk-based approach must be applied to business relationship monitoring, based notably on the customer's business and risk profile, and the grounds for suspicion have been broadened;
- supervision of compliance with AML/CFT provisions has been amplified and reorganized, notably reallocating all onsite and offsite banking supervision tasks to the OeNB; and

- savings deposit accounts review is incorporated into onsite supervisory examinations; credit institutions must inform the A-FIU of all requests to withdraw funds from savings deposits with a balance of at least EUR 15,000, when the identity of the customer has not been ascertained.

135. In addition, amendments to the legal framework have enlarged categories of higher risk customers to include PEPs and correspondent relationships, broadened the scope of activities related to the financing of terrorism, subjected money transmitters and exchange bureaus to the BWG provisions, and expanded preventive measures to additional categories of DNFBPs. The Austrian Federal Statute on the Responsibility of Entities for Criminal Offenses provides a general criminal liability for legal persons and entities for all penal offenses. Austria has ratified the Palermo Convention on 23 September 2004. In the area of international cooperation, the Vienna Convention has been ratified and implemented.

## 2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

### 2.1 Criminalization of Money Laundering (R.1 & 2)

#### 2.1.1 Description and Analysis

##### Legal Framework

136. In Austria, Article 165 of the StGB set forth the offense of Money Laundering (ML). The offense was established in 1993 and amended several times. Austria has signed and ratified the 1988 United Nations (UN) Convention on Illicit Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transnational Organized Crime (Palermo Convention).

##### *Criminalization of Money Laundering (c. 1.1—Physical and Material Elements of the Offense)*

137. Article 165 sets forth three different types of conducts that constitute the ML offense, all of which are largely in line with the material elements listed in Article 3(1) (b) and (c) of the Vienna Convention and Article 6(1) of the Palermo Convention:

- The first type applies to a person who intentionally conceals assets originating from a crime or a specified misdemeanor committed **by another person** (therefore excluding the case of self-laundering), or disguises their origin, particularly by providing false information in legal relations with regard to the true origin or nature of the assets, ownership or other rights, the right to dispose of the assets, their transfer or their location (Article 165, paragraph 1, covering Article 3, paragraph 1, b, ii of the Vienna Convention and Article 6, paragraph 1, a, ii of the Palermo Convention);
- The second type applies to whoever knowingly acquires such assets, holds them in custody, invests, administers, converts, realizes or transfers them to a third party (Article 165, paragraph 2). This broad range of activities covers not only the conversion and transfer but also the acquisition, possession and use (Article 3, paragraphs 1, b, i and 1, c, i of the Vienna Convention and Article 6, paragraphs 1, a, i and 1, b, i of the Palermo Convention);
- In addition to the material elements set forth in the Vienna and Palermo Conventions, Article 165 includes a third type of conduct, that applies to whoever knowingly, **acting on**

**behalf or in the interest of a criminal organization** (as defined in Article 278a of the StGB) **or a terrorist group** (as defined at Section 278b), acquires assets of that organization or group, holds them in custody, invests, administers, converts, realizes or transfers them to a third party (Article 165, paragraph 5). During the assessment, the authorities did not share a uniform view as to whether this provision would also cover the acts of members of the criminal organization (in which case there would be a partial derogation to the Austrian principle according to which ML may only be committed by a person other than the perpetrator of the predicate offense).

***The Laundered Property (c. 1.2)***

138. The offense of ML extends to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. Article 165 paragraph 4 of the StGB specifically provides that “a property item shall be deemed to derive from an offense when the perpetrator of the crime has obtained it through that offense or received it for the commission of that offense, or when it represents the value of the originally obtained or received property item.” It follows from this provision that the Austrian notion of proceeds covers any property that is the result of, or the reward for the crime, or the value thereof.

***Proving Property is the Proceeds of Crime (c. 1.2.1)***

139. The conviction of the offender for the predicate offense is not a necessary pre-condition to bringing charges for ML, although the prosecutors and judges met by the assessors indicated that when proving that property is the proceeds of crime, a conviction for the predicate offense is the best evidence that can be submitted. In any case, although the conviction for the predicate offense is not necessary to establish that assets were the proceeds of a predicate offense, the level of evidence required to prove the predicate offense (particularly in the case of the first two types of ML) is “beyond reasonable doubt.” This means that the prosecutor will have to prove the specifics of the predicate offense, for example, that the conduct amounted to a designated offense, the timeframe when the predicate offense was committed, the perpetrator, the types of assets that originated from the predicate offense, which is a rather high standard of proof. The various prosecutors and judges met by the assessors indicated that the standard of proof required to link ML to the predicate offense constitutes one of the most difficult obstacles (especially when the predicate offense was committed abroad). In case of laundering “in the interest of a criminal organization or of a terrorist group” (Article 165, paragraph 5), it is not necessary to link the ML activity to a specific predicate offense and it is sufficient to prove that the property laundered belongs to a criminal organization or a terrorist group. However, as indicated by the authorities, the conditions to prove that an associated group constitutes a criminal organization are also challenging.

***The Scope of the Predicate Offenses (c. 1.3)***

140. Predicate offenses for ML are all “crimes”, that is, offenses that are intentional acts punishable by life imprisonment or a term of more than three years (Article 17, paragraph 1 of the StGB), as well as a list of “designated misdemeanors” that include public corruption and bribery offenses, forgery of documents, criminal association as well as financing of terrorism. The list of misdemeanors was added in 2002. The range of penalties set forth in the StGB for these offenses does

not reach the threshold of three year imprisonment, consequently, these offenses would not have qualified as predicate offenses for ML without their specific inclusion in Article 165 StGB.

141. The list of predicate offenses to ML covers all the categories of offenses designated by the FATF, with the notable exception of counterfeiting and piracy of products, which is a misdemeanor in Austria and which is not included in the list of misdemeanors referred to in Article 165:

Statistical Table 8. Predicate offenses in Austria

<b>Designated categories of offenses in the Glossary to FATF 40</b>	<b>Predicate offenses explicitly mentioned in Article 165 StGB (designated list of misdemeanors)</b>	<b>Predicate offenses that are “crimes” (as defined by Article 17 StGB)</b>
Participation in an organized criminal group and racketeering	Article 278 StGB	Article 278a StGB.
Terrorism, including terrorist financing	Article 278b StGB, 278d StGB	Article 278d StGB.
Trafficking in human beings and migrant smuggling		Article 217 StGB, Article 104a StGB; Article 114 Aliens Police Act.
Sexual exploitation, including sexual exploitation of children		Article 201 et seq. StGB.
Illicit trafficking in narcotic drugs and psychotropic substances		Article 28 Act on Addictive Drugs, Article 28a Act on Addictive Drugs; Article 31 Act on Addictive Drugs; Article 31a Act on Addictive Drugs; Article 32 Act on Addictive Drugs.
Illicit arms trafficking		Article 177a StGB; Article 177b StGB.
Illicit trafficking in stolen and other goods		Article 164 StGB.
Corruption and bribery	Article 304 to 308 StGB	Article 302 StGB; Article 153 StGB.
Fraud		Article 147 StGB; Article 148 StGB; Article 148a StGB.
Counterfeiting currency		Article 232 StGB.
Counterfeiting and piracy of products	Not a predicate offense	Not a predicate offense.
Environmental crime		Article 180 StGB, Article 181 StGB, Article 181b – 181e StGB; Article 171 StGB, Article 172 StGB; Article 176 StGB, Article 177 StGB.
Murder, grievous bodily injury		Article 75 StGB, Article 76 StGB; Article 85 – 87 StGB.
Kidnapping, illegal restraint and hostage-taking		Article 99 StGB, Article 100 – 102 StGB.
Robbery or theft		Article 142, 143 StGB; Article 128 StGB; Article 129 – 131 StGB.
Smuggling;	Tax offense of smuggling or	

	evasion of import or export taxes (insofar as these fall within the competence of the courts)	
Extortion		Article 144, 145 StGB.
Forgery	Article 223, 224, 225, 229, 230 StGB.	
Piracy		Article 102 StGB; Article 142, 143 StGB; Article 144, 145 StGB.
Insider trading and market manipulation		Article 48b BörseG.

***Threshold Approach for Predicate Offenses (c. 1.4)***

142. As noted earlier, the predicate offenses to ML include all serious offenses under Austrian criminal law (“crimes” as stipulated by Article 17 of the StGB, that is, intentional criminal offenses punishable with more than three years of imprisonment), as well as a wide range of designated misdemeanors (which does not include counterfeiting and piracy of products).

***Extraterritorially Committed Predicate Offenses (c. 1.5)***

143. The Austrian authorities state that as a matter of principle they can establish jurisdiction for ML offenses irrespective of the place where the predicate offense was committed, as Austrian criminal law does not require that the latter offense be committed domestically, provided it would constitute a criminal offense under Austrian law. This view is reflected in the language of Article 165, Paragraph 1 (“... property items that derive from the crime of another person ...”) which does not limit the scope of the ML offense to domestic predicate offenses. Moreover, Article 64, Paragraph 1 (8) of the StGB explicitly provides ground for jurisdiction when it states that: “Austrian penal laws are applicable regardless of the penal laws which are valid for the scene of crime to the following offenses being committed abroad”, quoting explicitly the offense of ML, when the laundering activities are committed abroad and the predicate offense is committed in Austria. In addition, Article 65 of the StGB (“Criminal offenses committed abroad which are subject to prosecution only if they are liable to prosecution according to the laws which are valid for the scene of the crime”), states the general principle (Paragraph 3) that “it is sufficient that the offense is liable to prosecution according to Austrian law if there is no penal power at the place where the criminal act was committed.”

***Laundering One’s Own Illicit Funds (c. 1.6)***

144. Self-laundering is not criminalized in Austria as Article 165 limits the scope of the ML offenses to assets “that derive from the crime of **another** person.” ML undertaken by a person “acting on behalf or in the interest of a criminal organizations or the terrorist group” (Article 165, paragraph 5) could however amount to self-laundering in this specific case if the ML activity is undertaken by a member of the criminal organization or of the terrorist group.

145. The authorities explained this limitation by referring to the criminal law principle according to which an offender (i.e., the one having committed the predicate offense) cannot be additionally and separately punished for a “post-offense behavior” that relates to the proceeds of his/her own crime (principle of “*post factum delicti*”). According to this principle of Austrian criminal law, one

punishable act (the predicate offense) includes another concurring act (the concealing or disguising of property items that derive from the predicate offense's perpetrator) and the penalty set forth for the punishable act is deemed to cover the entire unlawfulness of the offenders' act. According to a further explanation given, the self-laundering activities are not considered to be subject to criminalization because they are deemed not to entail any additional damage to further rights than the one already caused by the predicate offense. In several rulings, the Supreme Court confirmed that the laundering activities undertaken by the perpetrator of the predicate offense do not constitute autonomous criminal activities, because they have to be seen as part of the "same historical happening" (which is interpreted in very broad terms in regard to the timeframe in which the predicate offense and the laundering activities are undertaken) of the predicate offense and they do not entail an autonomous and additional damage to vested rights, the protection of which is already ensured by the punishment of the predicate offense.

146. However, these rulings do not explicitly indicate that self-laundering is contrary to a fundamental principle of Austrian law and the officials met by the assessors did not have a uniform view as to whether there is a fundamental principle on the subject; it was pointed out that an amendment to the StGB could suffice to overturn this principle of criminal law. With respect to the "same historical happening" jurisprudence, one could argue -especially when the laundering activity does not simply amount to the mere possession or use, but also involves the transfer or the concealment and disguise through the financial system—that an additional damage to further rights than the one already caused by the predicate offense—as well as an additional social danger (to the soundness and the integrity of the financial system) can be envisaged autonomously. In light of the above, it was not established that the non-criminalization of self-laundering is supported by principles that amount to fundamental principles according to the FATF standards.

### ***Ancillary Offenses (c. 1.7)***

147. The Austrian criminal law provides for appropriate ancillary offenses to the offense of ML. Attempt (as well as "any participation in an attempt") is criminalized for all offenses by Article 15 of the StGB, therefore including for ML. Article 12 of the StGB ("Treatment of all participants as offenders") covers aiding and abetting, facilitating and counseling, for its broad language, as clarified by the authorities, states that "a criminal offense is committed ... also by anybody who abets another person to commit the offense or *who contributes to its perpetration in any other way.*" Article 3 (1) (c) iii of the Vienna Convention, that requires the criminalization of "publicly inciting or inducing others, by any means, to commit any of the offenses established in accordance with this Article [including ML]" is also covered by Article 12 of the StGB (if the incitement or the induction is for the specific offense of ML) and, more generally, by Article 281 ("Incitement to disobedience of laws") and 282 ("Incitement to criminal offenses and approval of criminal offenses"), in the case in which the incitement is generically to commit criminal offenses or to disobey laws.

148. Conspiracy to commit ML, in the sense generally known in common law systems (that envisage conspiracy also in the case of an agreement of only 2 persons), is not to be found in Austrian criminal law. Austria has a civil-law based criminal system and the basic concepts of such a system do not provide that such behavior constitutes punishable criminal conduct. Instead Austrian criminal law criminalizes "criminal association" (Article 278 of the StGB), as "a union planned for a longer time of more than two persons aiming at the commitment of one or more crimes", with a specific cross-reference to Article 165 of the StGB. This is in line with the Vienna and Palermo Conventions

(Article 3, paragraph 1, c, iv and Article 6, paragraph 1, b, ii, respectively, which require the establishment of an offense either for conspiracy or association, subject to the constitutional/basic concepts of the jurisdiction's legal system).

***Additional Element—If an act overseas which do not constitute an offense overseas, but would be a predicate offense if occurred domestically, lead to an offense of ML (c. 1.8)***

149. As noted earlier, Article 65, paragraph 3 of the StGB states the principle according to which “it is sufficient that the offense is liable to prosecution according to Austrian law if there is no penal power at the place where the criminal act was committed.”

***Liability of Natural Persons (c. 2.1)***

150. The Austrian criminal law knows three types of *mens rea* that characterize the offender's action (or inaction): “intentionally”, “willfully” or “knowingly” (Article 5 of the StGB).<sup>11</sup> The authorities explained that “intentionally” (*dolus*) is the broadest standard, for it includes also “*dolus eventualis*” (blind willfulness or recklessness, *bedingter Vorsatz*). When a criminal provision does not specify the *mens rea* required (as in the case of the first type of ML conduct, the one set forth by Article 165, paragraph 1), it is always assumed that the type of *mens rea* that applies is “intentionally.”

151. In the case of ML the *mens rea* requirements are differentiated according to the *modus operandi* of the ML offense: in the case of Paragraph 1 of Article 165 the act of concealing/disguise has to be committed with intent. In this case the *mens rea* is broader than that required by the Vienna and Palermo Convention, because it also includes *dolus eventualis*. Paragraph 2 of 165 requires that the acts of acquiring, converting, transferring, etc. be committed “knowingly.” This standard also appears to be broader than the one envisaged by the Vienna and Palermo Conventions, in the sense that it does not require the specific “purpose of concealing or disguising the illicit origin of property or of helping any person who is involved in the commission of the predicate offense to evade the legal consequences of his/her action” (Article 3, paragraph 2, b, i and Article 6, paragraph 1, a, I, respectively). Knowledge that the assets are proceeds of crime is sufficient.

***The Mental Element of the ML Offense (c. 2.2)***

152. Although the criminal law does not explicitly provide that the intentional element of the offense of ML may be inferred from objective factual circumstances, Austria relies on the principle of free evaluation of evidence by the judiciary, codified by Article 14 of the Criminal Procedure Code (*Strafprozessordnung, StPO*), which enables the judge to make this inference. As indicated by the

---

<sup>11</sup> (1) A person is behaving intentionally who wants to produce the facts constituting an offence under the law; to this end, it is sufficient that the offender seriously believes such production to be possible and that he resigns it. (2) The offender is behaving willfully when it is important to him that he produces those circumstances or results for which willful acting is a statutory prerequisite. (3) The offender is behaving knowingly when he not only believes the circumstances or result to be possible for which it is a statutory prerequisite that it is produced knowingly, but when he rather feels certain that such circumstance or result is either existent or that it will ensue.

authorities, the objective factual circumstances will very often be the most important clue for the judge's assessment of evidence.

***Liability of Legal Persons (c. 2.3)***

153. The Austrian Federal Statute on the Responsibility of Entities for Criminal Offenses (*Verbandsverantwortlichkeitsgesetz, VbVG*), which entered into force on January 1, 2006, provides for general criminal liability of legal persons and other entities such as commercial partnerships (*Personenhandelsgesellschaften*), private foundations or registered partnerships (*eingetragene Erwerbsgesellschaften*) for all criminal offenses (therefore including for ML), in addition to and independent from the liability of the natural persons prosecuted for the same act.

154. According to Article 3 of the VbVG, criminal liability is explicitly provided for an offense committed by a person with a leading position (“decision-maker”) on the one hand and for an offense by a person under its authority (“staff-member”) based on the lack of supervision or control of such a person in a leading position on the other. A legal person is responsible for a criminal offense (including ML) if either the offense was committed for the benefit of the entity or resulted from a neglect of the due diligence required of the entity. According to Article 3, paragraph 2 of the VbVG, the entity shall be responsible for offenses committed by a decision maker if the decision maker acted illegally and culpably.

155. In particular, according to Article 3, paragraph 2 of the VbVG, an entity is responsible for criminal offenses committed by a “decision maker” if he/she acted illegally and culpably, whereas in the case of its staff-member the legal person is responsible (paragraph 3) if:

- the facts and circumstances which correspond to the statutory definition of an offense have been realized in an illegal manner; and
- the commission of the offense was made possible or considerably easier due to the fact that decision makers failed to apply the due and reasonable care (diligence) required in the respective circumstances, in particular by omitting to provide for effective technical, organizational or staff related measures to prevent such an offense.

***Liability of Legal Persons should not preclude possible parallel criminal, civil or administrative proceedings (c. 2.4)***

156. As ML constitutes an offense under penal law also in the case of legal persons, administrative proceedings to address the conduct of legal persons or entities who may have engaged in money laundering offenses are not foreseen by the law. However, the criminal liability of legal persons or entities does not exclude civil liability which may result from the respective unlawful act.

***Sanctions for ML (c. 2.5)***

157. Penalties for ML vary based upon the amount of proceeds involved. The basic ML offenses defined at paragraphs 1 and 2 of Article 165 are misdemeanors and carry a maximum penalty of two

years of prison or a fine, which is calculated on daily rates<sup>12</sup> (the maximum amount for this fine equals to 360 daily rates). They become subject to a higher penalty ranging from six months to five years of prison when aggravated circumstances occur, that is when the assets involved exceed the value of EUR 50,000 or when the crime is committed as “a member of a criminal group associated for the purpose of continuous ML (Article 165, paragraph 3). The authorities clarified that this aggravating circumstance occurs also if the criminal association has carried out only one act of ML, as long as it can be ascertained at least that the purpose for which the association was established is “continuous ML”). In case of ML conducted “on behalf or in the interest of a criminal organization ... or terrorist group, the penalty is imprisonment for a term not exceeding three years (Article 165, paragraph 5). In this case, if the value of the assets exceeds EUR 50,000, the penalty goes up to a prison term ranging from six months to five years.

158. Article 4 VbVG provides for fines being imposed on legal persons. Similar to fines imposed on natural persons, the VbVG provides a daily rate system, in which the amount of the fine depends on two factors:

- Firstly, on the gravity of the offense, expressed by the maximum term of imprisonment of the offense provided by the penal law. Article 4 VbVG provides for a sliding scale from 40 to 180 daily rates based on the maximum imprisonment sentence, which can be imposed on natural persons for the offense in question. Thus, Article 4 of the VbVG provides a maximum fine of 70 daily rates for ML, which rises up to a maximum of 100 daily rates, if the ML offense is committed with regard to items worth more than EUR 50,000 or if it was committed as a member of a criminal group associated for the purpose of continuous ML or on behalf of the interest of a criminal organization or a terrorist group;
- Secondly, the amount of the fine depends on the revenue of the legal person or entity. The daily rate for a legal person shall be equal to one 360th of the yearly proceeds, reduced or augmented up to 30 percent taking into consideration its overall economic situation (Article 4, paragraph 4 of the VbVG). It is the court’s duty to assess the exact daily rate based on the profit situation and the financial performance of the legal entity.

159. The maximum daily rate is set at EUR 10,000 and the minimum daily rate, which is only relevant for entities that have not earned profit over a reasonable period of time, is EUR 50.

160. The authorities explained that the VbVG deliberately does not define the assessment basis for revenues or permissible deductions as a result of the broad coverage of all legal persons, which are generally subject to various accounting standards depending on their legal structure. On the other hand, the VbVG does not determinate the relevant time period for the calculation of profits. This provides some protection against manipulations of the amount of revenue. The current provision enables the court to average out the proceeds of the legal person or entity over several years, thus minimizing the risk of manipulating the amount of the fine by transferring gains of one given period to previous periods with losses.

---

<sup>12</sup> In the case of natural persons the minimum daily rate is equivalent to EUR 2 and the maximum to EUR 500.

161. The authorities explained that as the minimum daily rate has been fixed at EUR 50 and the maximum daily rate EUR 10,000, the minimum fine for the offense of ML committed by a legal person in the case of ML is EUR 3,500 and the maximum fine EUR 1,000,000.

162. Furthermore, Article 10 of the VbVG stipulates that the legal consequences shall also apply to a legal successor, if the rights and obligations of the legal person or entity have been transferred to another association by way of universal succession. Legal consequences imposed on the legal predecessor shall therefore also apply to the legal successor. If there are more than one legal successor, a fine imposed on the legal predecessor may be enforced vis-à-vis any legal successor. Other legal consequences may be attributed to individual legal successors to the extent that this is in line with their area of activity.

163. The sanctions set forth for ML in the case of natural persons and the minimum sanction established in the case of legal persons are too lenient (particularly in the case of basic ML) and do not seem effective, nor proportionate or dissuasive, especially considering that ML in most instances is not a crime but a simple misdemeanor. The authorities explained that, as a matter of criminal policy, ML is seen mostly as an ancillary offense and that prosecutors prefer to consider the ML activity as “participation” in the commission of the predicate offense (for the broad terms in which Article 12 is formulated, described above), which carries the same penalty as the predicate offense (usually higher than the one envisaged for ML) and may be easier to prove than ML (where, as mentioned earlier, it may be difficult to prove the link between ML and the predicate offense).

164. From a more general standpoint it has also to be noted that the relatively low penalties applied so far (see statistics) do not seem to constitute a strong deterrent to prevent ML activities.

### **Effectiveness**

165. While the ML criminal provision is largely in line with the material elements of the Vienna and Palermo Conventions, questions can be raised in regard to its effective implementation. One issue is that the number of convictions for ML under Article 165 (official statistics are available for 2004-2006 in the case of convictions; for conditional, unconditional and partially unconditional sentences statistics are also available for 2007)<sup>13</sup> is extremely low:

Statistical Table 9. Money Laundering Cases

	<b>ML cases – total</b>	<b>ML investigations (by public prosecutors)</b>	<b>ML prosecutions (dealt with by courts)</b>	<b>ML Convictions (as published by Statistics Austria)</b>
<b>2003</b>	29	17	12	7
<b>2004</b>	47	34	13	5
<b>2005</b>	24	20	4	3
<b>2006</b>	75	61	14	3

<sup>13</sup> After the on-site mission, the authorities indicated that in 2007, a total 149 ML cases were registered; thereof, 133 investigations by public prosecutors, 6 preliminary investigations by investigative judges and 10 cases with indictment for ML in 2007.

166. The authorities explained that these figures are not conclusive as in the Austrian system of criminal statistic, convictions are counted only in relation to convictions for the offense which has the highest punishment (which is hardly the case for ML, when it is concurrent with other crimes). Therefore, a conviction in the criminal statistics is counted once only, irrespective of the number of offenses underlying the conviction. So the official statistics for ML include only cases in which ML was the sole offense or the offense with the highest threat of punishment among other offenses proven, but they do not include the number of convictions where ML was proven among other offenses.

167. According to a separate statistic compiled by the A-FIU and based on the actual number of ML charges underlying a conviction (“effective number of convictions”), there were 12 ML convictions in 2003, 10 in 2004, 5 in 2005, 10 in 2006, and 18 in 2007.

168. Even so, the number of convictions still appears low, and raises an issue of effectiveness of the ML provisions, considering the statistics on convictions and investigations for the most serious predicate offenses that generate illicit proceeds, particularly drug-related offenses.

Statistical Table 10. Statistic of Convictions for Serious Offenses

FATF Serious Offenses	Number of Convictions			
	2004	2005	2006	2007
Participation in organized criminal group	10	28	17	19
Racketeering	57	59	46	52
Terrorism and terrorist financing	0	0	0	0
Trafficking in human beings and migrant smuggling	335	375	333	n.v.
Sexual exploitation and sexual exploitation of children	55	38	24	43
Illicit trafficking in narcotic drugs and psychotropic substances	5703	6127	5794	5435
Illicit arms trafficking	256	307	329	346
Illicit trafficking in stolen and other goods	391	409	389	437
Corruption and bribery	49	2	7	3
Fraud	3189	3261	3139	2981
Counterfeiting currency	102	113	63	94
Counterfeiting and piracy of products	9	7	15	5
Environmental crimes	11	9	7	7
Completed murder	24	28	33	34
Attempted murder	12	21	15	20
Grievous bodily injury	1423	1359	1239	1284
Kidnapping, illegal restraint and hostage-taking	55	72	61	44
Robbery	619	627	680	737
Theft	9480	9316	8523	8518
Smuggling	25	22	8	n.v.
Extortion	57	49	46	52
Forgery	564	502	538	493
Piracy	0	0	0	0
Insider trading	0	0	0	1

(source: Statistics Austria)

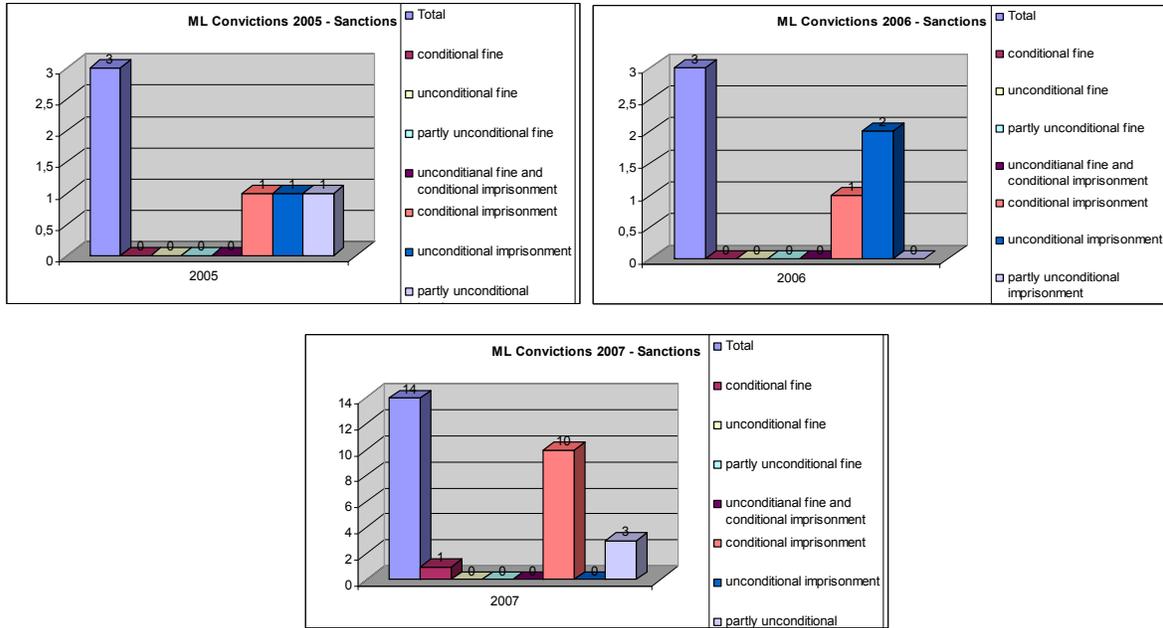
Statistical Table 11. Statistics on persons under investigation for the designated categories of offenses referred to by the Glossary (2006)

Designated Offenses	Section (StGB)	Number of Persons under Investigation
Participation in organized criminal group	§§ 278, 278a StGB	351
Racketeering	§§ 144, 145 StGB	345
Terrorism and terrorist financing	§§ 278b, c, d StGB	0
Trafficking in human beings and migrant smuggling	§§ 104a StGB, § 116 FPG bzw. §§ 104, 105 FremdenG 1997	10
Sexual exploitation and sexual exploitation of children	§§ 214, 215a, 216, 217 StGB	256
Illicit trafficking in narcotic drugs and psychotropic substances	§§ 27, 28, 30 - 32 SMG	23,444
Illicit arms trafficking	§ 50 Waffeng, § 7 KriegsmatG, § 177a StGB	1,088
Illicit trafficking in stolen and other goods	§ 164 StGB, § 37 FinStrG	1,321
Corruption and bribery	§§ 168c, d StGB, § 304 - 308 StGB	n.a
Fraud	§§ 146 - 148 StGB	18,583
Counterfeiting currency	§§ 233 - 236 StGB	375
Counterfeiting and piracy of products	§ 42 GebrauchsmusterG, § 22 HalbleiterschutzG, §§ 60, 68h MarkenschutzG, § 35 MusterschutzG, § 25 SortenschutzG	n.a
Environmental crimes	§§ 180, 181, 181b, 181c, 181d, 182, 183 StGB	143
Completed murder	§ 75 StGB	58
Attempted murder	§§ 15, 75 StGB	88
Grievous bodily injury	§§ 84, 85, 86, 87 StGB	3,269
Kidnapping, illegal restraint and hostage-taking	§§ 99, 100, 101, 102 StGB	391
Robbery	§§ 142, 143 StGB	2,346
Theft	§§ 127 - 131 StGB	46,415
Smuggling	§ 35 FinStrG	n.a.
Extortion	§ 144, 145 StGB	345
Forgery	§§ 223, 225, 225a, 237, 238, 241a, 293, 311 StGB	6,165
Piracy	§§ 185, 186 StGB	n.a
Insider trading	§ 48b BörseG	n.a

169. The authorities further indicated that the low figures can be explained by the lack of criminalization of self-laundering in Austria and by the fact that the prosecutors prefer to indict the ML activities under “participation”, because by doing so, they can apply the higher penalty provided in the case of participation in the predicate offense and, in practice, it is easier to prove participation in the predicate offense than the ML activity as a stand-alone crime.

170. However the assessors are of the view that criminalizing basic ML as a misdemeanor (therefore perceived as a low-danger offense) and the difficulties encountered by the prosecutors in proving the predicate offense have a significant influence in the low number of convictions.

171. In addition, penalties provided for these convictions were extremely low, (according to the official statistics for 2004–2007, which, as explained above, are compiled for the case where ML was convicted with the higher terms). The most severe penalty imposed was imprisonment for 1 to 3 years, in a case judged in 2006.



Statistical Table 12. ML Convictions 2004–2007  
Conditional, Unconditional and Partly Unconditional Fines

	Conditional Sentences				Unconditional Sentences			
	2004	2005	2006	2007	2004	2005	2006	2007
Imprisonment up to 1 Month	0	0	0	1	0	0	0	0
Imprisonment 1 to 3 Months	2	1	1	1	0	0	0	0
Imprisonment 3 to 6 Months	1	0	0	3	0	0	1	0
Imprisonment 6 to 12 Months	0	0	0	5	0	1	0	0
Imprisonment 1 to 3 Years	0	0	0	0	0	0	1	0
Imprisonment 3 to 5 Years	0	0	0	0	0	0	0	0
Imprisonment over 5 Years	0	0	0	0	0	0	0	0
Fine 60 to 120 Daily Rates	0	0	0	1	0	0	0	0

Statistical Table 13. ML Convictions 2004–2007  
Sentences for Imprisonment

	2004	2005	2006	2007
Section 12 Juvenile Court Act (JGG)	1	0	0	0
Partly Unconditional Imprisonment	1	1	0	3

### 2.1.2 Recommendations and Comments

172. The authorities should:

#### Recommendation 1

- Criminalize self-laundering;
- Undertake actions (awareness raising or training) that would alter the kind of proof currently deemed necessary to show that property is proceeds or that conduct resulted in proceeds so that it will not be necessary for a successful prosecution that the prosecutor provide evidence that a specific offence occurred or a specific perpetrator engaged in the conduct; and
- Make counterfeiting and piracy of products predicate offenses to ML.

#### Recommendation 2

- Increase the penalties set forth for natural persons by Article 165 and the minimum sanctions applicable in the case of legal persons.

### 2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	LC	<ul style="list-style-type: none"> <li>• No confirmation that the non-criminalization of self-laundering is supported by principles that amount to fundamental principles according to the FATF standard.</li> <li>• Low number of convictions and indictments for ML compared to the number of ML criminal investigations and convictions for serious offenses that generate proceeds in Austria, and standard of proof required by the courts to establish that assets originate from crime indicating an issue of effectiveness in the implementation of the ML criminal provision.</li> <li>• Counterfeiting and piracy of products not predicate offenses for ML.</li> </ul>
R.2	LC	<ul style="list-style-type: none"> <li>• Sanctions for ML against natural persons and minimum sanction established in the case of legal persons too lenient and not effective, proportionate or dissuasive.</li> <li>• Low number of convictions and indictments for ML compared to the number of ML criminal investigations and convictions for serious offenses that generate proceeds.</li> </ul>

## 2.2 Criminalization of Terrorist Financing (SR.II)

### 2.2.1 Description and Analysis

#### Legal Framework

173. The financing of terrorism (FT) was criminalized in Austrian law by Article 278d of the StGB in 2002 on the basis of the International Convention for the Suppression of the Financing of Terrorism (ICSFT).

***Criminalization of Financing of Terrorism (c. II.1)***

174. Article 278d of the StGB (“Financing of terrorism”) states the following:

- “(1) A person who provides for assets or collects them with the intent that they are used for the commitment:
1. of a hijacking (Article 185) or an intentional danger to the safety of aviation (Article 186);
  2. of an extortionate kidnapping (Article 102), or the threat with it;
  3. of an attack on life and limb or the freedom of a person protected by international law or a violent attack on an apartment, the official premises or the means of transportation of such a person which is appropriate to expose this person to a danger to life and limb or freedom or a threat with it;
  4. of an intentional endangering by nuclear energy or ionized radiation (Article 171) or a threat with it, of a unlawful use of nuclear materials or radioactive substances (Section 177b), of any other criminal offense to obtain nuclear materials or radioactive substances or of the threat to commit a theft or robbery of nuclear materials or radioactive substances aiming to force another person to an action, permission or omission;
  5. of a considerable attack on life and limb of another person on an airport serving the international civil aviation, of an destruction or considerable damaging of such an airport or a civil aircraft being on it or an interruption of the services on the airport, so far as the offense is committed by the use of a weapon or other device and is appropriate to endanger the security of the airport;
  6. of a criminal offense committed in a way mentioned in Arts. 185 or 186 against a vessel or a fixed platform, against a person being on board of a vessel or a fixed platform or against the cargo loaded on a ship or an equipment of the ship;
  7. of the transportation of a blasting composition or another deadly device in a public place, to a governmental or public institution or a public traffic system or services of supply or of the operation of these means aiming to cause the death or a grievous bodily injury of another person or the destruction of the place, institution or system to a high degree, as far as the destruction is appropriate to bring about a considerable economic damage;
  8. of a criminal offense which shall effect the death or a grievous bodily injury of a civil person or another person not being actively involved in the hostilities of an armed conflict if this act is aimed by the reason of its nature and the circumstances at threatening a group of the population or forcing a government or an international organization to an action or omission; is to be sentenced to imprisonment from six months to five years. But the nature and extent of the sentence must not be severer than the penalty provided for the financed offense.

- (2) The offender shall not be punished under paragraph 1 if the offense is subject to a severer penalty under another provision.”

175. This provision, largely in line with Article 2 of the 1999 ICSFT, criminalizes the provision or collection of assets with the intent that such assets be used for committing one of the listed offenses, including hijacking, kidnapping for ransom, offenses against internationally protected persons, offenses involving misuse of nuclear material, offenses against airport staff or material, offenses against the safety of navigation, terrorist bombing or any other terrorist offense against civilians in armed conflicts. The offenses listed by Article 278d mirror the offenses which fall within the scope of the nine international treaties appearing in the annex to the ICSFT and the language of Article 2, Paragraph 1 (b) of the ICSFT and thus fully cover the FT offense defined under its Article 2, Paragraph 1.

176. The StGB has also a separate provision (Article 278c) which criminalizes the commission of terrorist criminal offenses.<sup>14</sup> These acts are series of offenses set forth by the StGB or by special laws and coincide to a certain degree with the list of offenses referred to by the FT provision; when they amount to acts of terrorism, the maximum punishment which is set forth for the offenses by the specific provisions of the StGB is increased by half, but it cannot exceed 20 years of imprisonment.

177. As previously noted, the FT offense of Article 278d technically refers to the offenses set forth by Article 2, paragraph 1 of the ICSFT rather than to those listed in the StGB (Article 278c). This distinction is relevant for the following reason: Article 278c, paragraph 3 introduces an exclusion of criminality for the offenses considered as terrorist acts listed in Paragraph 1, because it states that “the offense is not regarded as terrorist criminal offense if it is directed to the establishment or re-establishment of a democratic and constitutional situation or the exercise or observance of human rights.” In this case, the offenses are not considered “terrorist criminal offenses” under Article 278c and are punished according to the penalties set forth by the specific provisions of the StGB. This exclusion of criminality, which was criticized by the UN Sanction Committee, although not

---

<sup>14</sup> According to Article 278c, paragraph 1, terrorist criminal offenses are:

1. murder (Section 75),
2. bodily injuries under sections 84 to 87,
3. extortionate kidnapping (Section 102),
4. gross intimidation (Section 106),
5. dangerous threat (Section 107, paragraph 2),
6. gross damage to property (Section 126) and damaging of data (Section 126a) if thereby a danger to the life of another person or a danger to the property of another person to a large extent can be caused,
7. intentional offences of dangerousness to public safety (Sections 169, 171, 173, 175, 176, 177a, 177b & 178) or intentional infringement of environment (Section 180),
8. hijacking (Section 185),
9. intentional danger to the safety of aviation (Section 186), or
10. a criminal offence punishable under section 50 of the Weapons Act 1996 or section 7 of the War Material Act, if the offence is appropriate to cause a severe interference with the public life or such an interference for a longer time or to cause a severe damage to the economic life being committed with the intent to intimidate the people in a serious manner or to force public authorities or an international organization to an action, permission or omission or to convulse or destroy the political, constitutional, economic or social basic structures of a state or an international organization.

technically applicable to the case of FT (because Article 278d does not cross refer to 278c), has some cascading effects on other elements of SR.II, discussed below.

178. Article 278d does not explicitly indicate whether the indirect provision/collection also constitutes FT, but the authorities clarified that this case would nevertheless trigger criminal responsibility under Article 278d. They quoted a case, currently pending at the stage of pre-trial, which involved the indirect collection of money through an organization which was then providing the funds collected to another organization situated in a conflict zone.

179. The prosecutors and judges met by the assessors also confirmed that the offense does not require that the funds be linked to a specific terrorist act, nor that a terrorist act is committed or even attempted; being sufficient the provision or collection of the funds or other assets with the intent they are intended to be used or they will be used for the commission of a terrorist act.

180. The term “assets of property” includes any funds in the term defined by the ICSFT, including funds from a legitimate or illegitimate source.

181. Attempt (including “participation in an attempt”) is criminalized for all offenses, including FT, in Article 15 of the StGB. The types of conduct set out in Article 2, paragraph 5 of the ICSFT - participation as an accomplice, organization and direction of others, contribution to the commission of the offense by a group of persons acting with a common purpose- are covered by Article 12 (“Treatment of all participants as offenders”) and 278b of the StGB (“Terrorist Association”) -though not in all instances. Article 12 covers participation as an accomplice, as it states that “a criminal offense is committed not only by the immediate perpetrator that commits the criminal offense but also by anybody who abets another person or who contributes to its perpetration in any other way.”

182. Organization and direction of others (in regard to the commission of terrorist acts) trigger criminal responsibility for “terrorist group” and in particular for “leading a terrorist association” (Article 278b, paragraph 1). A “terrorist group” is defined as a “union planned for a longer time of more than two persons aiming at the commitment of one or more terrorist criminal offenses—listed by Article 278c—by one or more members of the group. However, the scope of this provision is limited by the exclusion of criminality contained in paragraph 3 of Article 278c, in the sense that if the union is planned for the commission of acts listed in 278c but for the purpose of the establishment or re-establishment of a democratic and constitutional situation or the exercise or observance of human rights”, it will not qualify as a “terrorist group.”

183. More complicated is to envisage criminal responsibility for organization and direction of others, as well as contribution to the criminal activities committed by a group of persons acting with a common purpose when the organization and direction of others or the contribution are only in regard to FT (and not to the commission of terrorist acts). It appears that a group established for the sole purpose of FT is not subject to the criminal responsibility set forth in the case of a “terrorist group” under Article 278b, because of the reference to the acts indicated by Article 278c (which do not include Article 278d) as a qualifying element for the constitution of the offense. Nor can such criminal responsibility always be envisaged by applying Article 278 (Criminal association because when FT is a misdemeanor (i.e., when the act of FT is not punished with more than three years of imprisonment), it is not included in the list of misdemeanors which constitute one of the material elements of the criminal association.

184. The offense of FT as defined by Article 278d of the StGB adequately covers the material elements set out in Article 2, paragraphs 1, a and b and paragraph 5, a of the ICSFT, but it does not cover in all instances the direction and organization of others and the contribution to a group of persons acting with a common purpose (as required by Article 2, paragraphs 5, b and c, when organization/direction is solely for FT and when the group of persons has only FT as a common purpose).

185. The offense of FT is also not entirely consistent with SR.II in the sense that it does not fully cover the financing of terrorist organizations and the financing of the individual terrorist regardless of whether that financing is for criminal activities, legal activities or general support. The provision/collection of funds for a terrorist organization or for the individual terrorist would not amount to a criminal offense unless it can be established that the perpetrator knew (also by the broader standard of the *dolus eventualis*, which is applicable in the case of FT, as discussed later) that the funds are intended to be used or will be used for the commission of a terrorist act as defined by Article 278d.

186. In the case of financing of a terrorist association, the authorities are of the opinion that Article 278b, paragraph 2, in combination with Article 278, paragraph 3, provides ground for the criminalization of financing the terrorist organization *per se*, regardless of whether that financing is for committing terrorist acts, criminal activities, legal activities or general support. Article 278b, paragraph 2 criminalizes the participation in the terrorist association as a member, and for the definition of “member” it refers to Article 278, paragraph 2. Indeed this provision criminalizes in broad terms as “member participation in a criminal association” whoever participates in the association’s activities “by providing assets or in another way with the knowledge that he/she promotes thereby the association or its criminal acts.” The authorities maintain that the mere provision of funds or other assets with the aim of promoting the association or its acts would be sufficient to constitute the offense of “participation as a member” in the association, and to apply the relevant punishment. They state that, *mutatis mutandis*, this can also be applied to the provision/collection of funds for a terrorist association, even in the case of a single act of provision/collection. However, the exception of criminality set forth in paragraph 3 of Article 278c would constitute an impediment to pursue the financing of a terrorist association (or the individual terrorist) in the sense indicated by the authorities (participation as a member), because if the acts are committed for one of the purposes indicated in these provisions, they are not deemed as terrorist acts and, consequentially, an association established for these purposes would not be considered a terrorist association.

187. The financing of the individual terrorist regardless of whether that financing is for committing terrorist acts, criminal activities, legal activities or general support can only trigger criminal responsibility if it can be proved that the financier was at least aware that the funds were meant to be used or intended to be used for the commission of a terrorist act (including if the knowledge is in the form of *dolus eventualis*: the authorities indicated the example in which the financier accepted the possibility that the person could be part of a dormant terrorist cell, in which case this would suffice to trigger the criminal responsibility for FT).

***Predicate Offense for Money Laundering (c. II.2)***

188. The FT is a predicate offense to ML, as Article 165 of the StGB (“Money Laundering”) explicitly cross-references to Article 278d (“Financing of Terrorism”).

***Jurisdiction for Terrorist Financing Offense (c. II.3)***

189. FT offenses apply regardless of whether the person alleged to have committed the offense(s) is in the same country or a different country than the one in which the terrorist(s)/terrorist organization(s) is located or the terrorist act(s) occurred/will occur. As mentioned earlier, a case which is currently in a pre-trial phase involves the collection and provision of funds through an organization in a third country that is experiencing a conflict.

190. The FT offense applies if the provision or collection of assets takes place in Austria, irrespective of the place where the terrorist act is, or is planned to be committed. If the FT offense itself was committed abroad, according to Article 64, paragraph 1(10), Austria may have jurisdiction only if: (i) the perpetrator was Austrian at the time of the offense or he/she has gained the Austrian citizenship afterwards and is still in its possession at the time of the institution of criminal proceedings; or (ii) the perpetrator was a foreigner at the time of the offense, but is in Austria at the time of prosecution and cannot be extradited.

***The Mental Element of the FT Offense (applying c. 2.2 in R.2)***

191. The criterion is met.

***Liability of Legal Persons (applying c. 2.3 & c. 2.4 in R.2)***

192. The criterion is met.

***Sanctions for FT (applying c. 2.5 in R.2)***

193. The penalty that the FT offense carries is a prison term ranging from six months to five years, but the sentence imposed must not exceed the penalty provided for the financed offense and the offender will be punished to a more severe penalty if the FT is subject to a more severe penalty under another provision. The authorities explained, regarding the principle of penalty equation with the financed offense or its total consumption by a more severe penalty, that this derives from the accessory nature of the FT offense, which would normally be regarded as an act of aiding and abetting and thus would, under general criminal law principles, carry exactly the same penalty as the main offense. However this may create an issue with respect to the specificity of the financed offense (considering that, according to the international standard, there should not be a specific linkage between the financing and a specific terrorist act).

194. Legal persons can also be held criminally responsible for FT. Article 4 of the VbVG provides for a maximum fine of 100 daily rates for the offense of FT. Therefore, the maximum fine for FT for legal persons and entities is—as it is for ML—EUR 1,000,000.

195. The sanctions for natural persons appear to be too low, both in their minimum and their maximum, and therefore are not effective, nor proportionate or dissuasive.

**Implementation and Effectiveness**

196. The statistics available only show the number of investigations on FT cases. The authorities informed the assessors that between 2003 and 2006, 18 criminal cases related to FT were registered, but none of them led to an indictment (see breakdown below). In 16 cases, the proceedings were dismissed by the public prosecutors. In 2007, four FT cases were registered (two criminal investigation by public prosecutors and two preliminary investigations by investigative judge). Three of them have been terminated, one case is still pending. The authorities also reported that there was no conviction for FT between 2004 and 2007.

197. In 2003, four criminal cases related to FT were registered: criminal investigations were conducted by public prosecutors in three cases and a preliminary investigation was conducted by an investigative judge in the fourth. In 2004, five FT cases were registered: criminal investigations were conducted by public prosecutors in four cases and a preliminary investigation was conducted by an investigative judge in the fourth case. In 2005, three criminal investigations were led by public prosecutors. In 2006, six criminal investigations were conducted by public prosecutors and two preliminary investigations were led by investigative judges.

198. On March 12, 2008, a court sentenced a couple in Austria on the basis of charges of membership in a terrorist association (*Al-Qaeda*), threatening the Austrian Government, as well as attempted coercion for producing video promoting *Al-Qaeda*. The Supreme Court annulled the verdict on procedural grounds and remitted it to the court for re-examination.

199. The authorities deem the risk of FT in Austria low, compared with other European jurisdictions; the existence of 18 criminal investigations since 2003 show attentiveness to the risk that FT may pose.

### 2.2.2 Recommendations and Comments

200. The authorities should:

- extend the criminalization of FT in all instances envisaged in SR.II with reference to the financing of terrorist organizations and the individual terrorist, regardless of whether that financing is for criminal activities, legal activities or general support;
- extend the criminalization to the whole range of activities envisaged by Article 2, paragraph 5 (b) and (c) of the 1999 UN Convention; and
- increase the penalties set forth for FT.

### 2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	PC	<ul style="list-style-type: none"> <li>• The offense of FT not fully applicable in all the circumstances envisaged by SR.II, because in the case of the financing of a terrorist organization or an individual terrorist, the provision and collection of funds <i>per se</i> may not constitute an offense if it cannot be established that the provision or collection was with the knowledge that the assets were intended to be used for the commission of terrorist acts and in some other circumstances.</li> </ul>

	<ul style="list-style-type: none"> <li>• Penalties too low and possible need for a link to a specific offense for penalty purposes.</li> <li>• Criminalization of organization and direction of others not fully in line with the 1999 UN Convention.</li> </ul>
--	--

## 2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

### 2.3.1 Description and Analysis

#### Legal Framework

201. The Austrian criminal law provides for two possibilities to confiscate property that has been laundered or which constitutes proceeds of any ML, FT or other predicate offense: confiscation of profits ("*Abschöpfung der Bereicherung*", Article 20 of the StGB) and forfeiture ("*Verfall*", Article 20b of the StGB).

202. In addition, a third possibility is offered for the removal of instrumentalities used in and intended for use in the commission of any ML, FT or other predicate offense. For these, Article 26 of the StGB (confiscation, "*Einziehung*") provides the confiscation of "objects which have been used or have been intended to be used to commit an offense or have been produced by this offense" if this is necessary to counteract the commitment of offenses.

203. Confiscation of profits applies to economic benefits derived from any criminal offense, whereas forfeiture to property being at the disposal of a criminal organization (Section 278a) or a terrorist group (Section 278b), or property that has been provided or collected as a means for financing of terrorism (Section 278d). In the latter case, property can be forfeited, even if it derives from an offense where Austrian jurisdiction does not apply, if the offense is punishable under the law of the State where it was committed. According to Article 65a of the StGB confiscation and forfeiture "apply to all property items in Austria."

204. The decision of confiscation or forfeiture can be made either as part of the main criminal trial (if any) or separately (Sections 443, 445 and 445a of the StPO: in the case in which there is no conviction but sufficient grounds for an offense, the prosecutor can initiate another proceeding for confiscation or forfeiture).

#### ***Confiscation of Property related to ML, FT or other predicate offenses including property of corresponding value (c. 3.1) and Confiscation of Property Derived from Proceeds of Crime (c. 3.1.1 applying c. 3.1)***

205. As mentioned above, in the Austrian criminal law "confiscation of profits" and "forfeiture" are provided in regard to property that has been laundered or which constitutes proceeds of ML, FT and other predicate offense. These measures apply to property that is derived directly or indirectly from proceeds of crime, including income, profits or other benefits from proceeds of crime, regardless of whether the property is held or owned by a third party. "Confiscation of profits" is value-based, so it also applies to property of corresponding value. For instrumentalities used in and intended for use

in the commission of ML, FT or other predicate offense, “confiscation” will apply as set out by Article 26 of the StGB.

### **Confiscation of Profits (Article 20 of the StGB)**

206. Confiscation of profits applies to a person who has committed an offense (including misdemeanors) and has obtained economic benefit from it, or has received economic benefit for committing an offense. The language used by the provision requires an illegal act only in objective terms, as a result of which the punishability of the offender is irrelevant for the confiscation of profits. The Austrian regime of confiscation of proceeds is value-based, so the person subject to confiscation under Article 20 will be issued a court order to pay an amount of money equivalent to the illegal profits gained. If the extent of the profits cannot be established at all, or cannot be established without disproportionate expenditure, the court may fix the sum of money to be confiscated according to its conviction.

207. Furthermore, under Article 20 the court may confiscate property that cannot be directly linked to a specified offense, based on a rebuttable legal presumption that benefits a defendant holds derive from other, non-identifiable offenses. This partially reverses the burden of proof. In this case there is no need for the prosecutor to prove that the money is the proceeds of a specific offense. This applies with regard to:

- A perpetrator who has committed *crimes* (according to Article 17 of the StGB; therefore not in the case of ML, which is a misdemeanor) continuously or repeatedly and has obtained economic benefits from, or received for their commission and has gained during the same period further economic benefits. The statute provides that for such additional economic benefits, there is “an obvious presumption that these benefits derive from other crimes of the same nature.” With the legal acquisition of the benefits not being made credible, these economic benefits have to be taken into consideration in fixing the amount of money to be confiscated (Article 20, paragraph 2);
- A perpetrator who belongs to a criminal organization (Article 278a) or a terrorist group (Article 278b) and who, during the period of his membership, has gained economic benefits is to pay the amount of gained profits “if there is an obvious supposition that these profits derive from offenses and their legal acquisition cannot be made credible” (Article 20, paragraph 3). This applies in the case of ML.

208. Under Article 20, paragraph 4, the value-based confiscation regime also covers third persons that benefit illegally and directly from an offense committed by another person, or from the economic benefit given for the commission of such an offense, as such persons may also be ordered to pay an amount of money equivalent to these profits. This applies *mutatis mutandis* to legal persons and partnerships that have gained profits. If the person who has gained illegal profits has died, or if the legal person or partnership has ceased to exist, the profits are to be confiscated from the legal successor insofar as they were still existent at the moment of transmission of rights (paragraph 5).

### **Forfeiture (Article 20b of the StGB)**

209. Criminal forfeiture applies in two cases, namely when:

- the property is at the disposal of a criminal organization (Article 278a) or a terrorist group (Article 278b), or has been provided or collected as a mean for financing terrorism (Article 278d);
- the property derives from an offense where Austrian criminal jurisdiction is not established under Sections 62–65, but the offense is punishable under the law of the State where it was committed.

210. The forfeiture provision at Section 20b is aimed specifically at forfeiting property at the disposal of criminal organizations or terrorist groups (defined in Articles 278a and 278b). Such forfeiture does not require prior conviction, but the existence of a “criminal organization” or of a “terrorist group” has to be established and proved. This type of forfeiture has been very rarely applied, because, as indicated by the authorities, of the difficulty to prove the elements of a “criminal organization.” According to Article 278a, “criminal organization” is defined as an “association of a considerable number of persons, intended to last a longer period of time and similar to an enterprise.” The elements that constitute this crime include (as in the case of criminal association) any activity done in relation to the organization regardless of whether or not the action in and of itself is a crime. However, in the case of “criminal organization” the several conditions set out in Article 278a must exist simultaneously in order to fulfill the elements of the crime: the criminal organization has to be designed to exist for a longer period of time (indefinitely or at least for several weeks; the case law says at least about three months); the union has to be constructed “similarly to an enterprise”, which implies division of labor (for example into planning and implementation), hierarchical structure (that some have the authority to give directives and that others have to follow directives) and a specific existing infrastructure (for example organizational capabilities). The “considerable number of persons” has been defined in case law as meaning ten persons or more.

211. Forfeiture can also be applied to property “abandoned” in Austria and derived from an extraterritorial offense over which Austria has no jurisdiction but is punishable under the law of jurisdiction where it was committed. Authorities explained that this provision also covers the case in which the property is indirectly held by the criminal organization or terrorist association (as in the case of a straw-man); the main requirement is to prove that the property (which can be any type of property) is at “the disposal” of the criminal organization/terrorist association.

### **Confiscation (Article 26 of StGB)**

212. According to this provision, which deals with instrumentalities, “Objects which have been used or have been intended to be used by the perpetrator to commit an offense or have been produced by this offense shall be confiscated, if the confiscation seems to be required by the special condition of the objects to counteract the commitment of offenses.” This provision allows for the confiscation of instrumentalities that are “objects”, not money which is subject to confiscation under Article 20 or forfeiture if it is at the disposal of the criminal organization/terrorist group. Confiscation of instrumentalities is also possible in the absence or a conviction or if the person cannot be subject to prosecution, as explicitly stated by Article 26, paragraph 3.

213. There are several exclusions from confiscation, confiscation of profits and forfeiture:

- In the case of confiscation of profits, these are when the defendant has satisfied any civil claims, or when the amount of money to be confiscated or the chances to enforce the

confiscation are disproportionate to the cost of enforcing it, or if the order would cause an inappropriate hardship to the person who gained the profit (Article 20a);

- In the case of forfeiture, these exclusions include legitimate claims by parties who have not participated in the offense, the criminal organization or terrorist group, as well as grounds that a foreign confiscation decision has already been made that can be executed in Austria or that forfeiture would be disproportionate to the importance of a matter or the expenditure involved in recovering it (Article 20c);
- In the case of confiscation of instrumentalities, it is to be refrained from the confiscation, if the person in question removes the special conditions that make an object useful in the commitment of an offense, especially if he/she removes or disables the devices or indications which facilitate the commitment of offenses. Objects which are legitimately claimed by a person not having participated in the offense shall only be confiscated if the person concerned does not guarantee that the objects will not be used to commit offenses.

### ***Provisional Measures to Prevent Dealing in Property subject to Confiscation (c. 3.2)***

214. Provisional measures are provided for in Articles 109-115 of the StPO. These are “Seizure” (*Sicherstellung*, Article 110 of the StPO) and “Sequestration” (*Beschlagnahme*, Article 115 of the StPO). In addition to these measures, the A-FIU has the authority to block ongoing or to postpone imminent transactions that are reasonably suspected of serving the purpose of ML or FT, under various laws.

### **Seizure**

215. According to Article 109-110 of the StPO, seizure consists of a temporary constitution of authority to dispose on objects, the prohibition to surrender objects or other assets to third parties and the prohibition to sell or pledge such objects and values, if these objects or assets are required for evidentiary purposes, or for securing civil claims, confiscation of profits (Article 20 of the StGB), forfeiture (Article 20b of the StGB), confiscation (Article 26 of the StGB) or any other order relating to property rights provided for in the law. Seizure is ordered by the office of the public prosecution and is executed by the criminal police (Article 110, paragraph 2). In certain instances (Article 110, paragraph 3)<sup>15</sup>, the criminal police is entitled to seize objects at its own discretion, but has to report to

---

<sup>15</sup> “The criminal police is entitled to seize objects at their own discretion (Section 109, n° 1, lit. a)

1. If they:

- Are under nobody’s authority to dispose.
- Have been taken from a victim of a criminal act.
- Have been found on the crime scene and could have been used or determined to be used for committing the criminal act. Or
- Are of low value or can be easily substituted for a limited period of time.

2. If their possession is generally prohibited (Section 445a, paragraph 1).

3. That are in the possession of a person arrested for reasons of Section 170 paragraph 1 no. 1 when arrested or that are found during a search according Section 120, paragraph 1. Or

4. In the cases of Article 4 of the Council Regulation (EC) no. 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights.”

the office of public prosecution immediately and at the latest within 14 days from the seizure (Article 113, paragraph 2).

### **Sequestration**

216. According to Articles 109 and 115 of the StPO, sequestration consists of a decision of the court to constitute or continue a seizure order, and in the prohibition, also ordered by a court, “to alienate, encumber or pledge real estates or rights listed in a public register” (Article 109, paragraph 2b). The sequestration is admitted if the objects seized presumably are required as evidence in a subsequent proceeding, are subject to civil law claims or will be needed to ensure a judicial decision on the confiscation of proceeds of crime, on forfeiture, on confiscation, or on any other order relating to property rights provided for in the law whose execution would otherwise be endangered or made considerably more difficult. Upon request of the office of public prosecution the court has to decide “immediately” about the sequestration.

217. Since Austria’s confiscation system is value-based and the purpose of the provisional measures is to safeguard any eventual value-based confiscation order, the seizure and sequestration can apply to legal, as well as illegal, property; in the case where seizure/sequestration are ordered to secure a judicial decision on the confiscation of proceeds of crime or forfeiture, an amount of money that will cover the presumable confiscation of proceeds of crime or the presumable forfeiture will have to be determined (Article 115, paragraph 5).

218. It has to be noted that, according to Article 110, paragraphs 4 and 115, paragraph 3 the seizure and the sequestration of objects for reasons of evidence is not admitted and in any case has to be terminated if the affected person requests it, “if and as soon as the aim of the evidence can be met with picture, sound or other recordings or with copies of written documents or data processed automation-aided and if there is no reason to assume that the seized objects themselves or the original versions of the information seized will have to be inspected during the court proceeding.”

### **A-FIU’s Power to Stop Transactions (Preliminary Injunction “*Anordnung*”)**

219. In addition to seizure and the sequestration, another provisional measure available in the Austrian system is the power of the A-FIU to block an ongoing or postpone the execution of an imminent transaction reasonably suspected of serving ML or FT. This power is set forth in Article 41, paragraph 3 of the BWG, Article 98f, paragraph 3 of the VAG and Articles 6 & 12, paragraph 4 of the WAG (similar provisions are contained in the legal acts for the remaining financial sector and the DNFBPs). According to these provisions, financial institutions and DNFBPs are obliged to inform the authorities without delay about transactions suspected of ML/FT. In such cases, the further execution of the transaction has to be stopped unless there is a risk that a delay in the transaction would complicate or obstruct investigations (Article 41, paragraph 1 of the BWG, Article 98f, paragraph 1 of the VAG, Articles 6 and 12, paragraph 4 of the WAG). The transaction can only be executed at the end of the following business day, unless otherwise instructed by the A-FIU.

220. If the A-FIU deems it appropriate, it can order the financial institution/DNFBPs not to execute the transaction. In this case, the A-FIU has to notify the client and the prosecutor forthwith upon taking such a measure. The notification of the client must contain the information that he/she, or any other thereby affected individual/entity, is entitled to file a complaint with the Independent

Administrative Court for violation of his/her rights. The A-FIU will have to lift the order as soon as the reasons for blocking or postponing the transaction no longer exist, or when the prosecutor rules that the preconditions for confiscation, as defined in Article 109, no. 2 and 115, paragraph 1, no. 3 of the StPO no longer exist (these are the conditions for applying sequestration). Otherwise such a blocking or postponing order taken by the A-FIU expires 6 months after being issued or when a court imposes sequestration pursuant to Article 109, no. 2, and 115, paragraph 1, no. 3, of the StPO (Article 41, paragraph 3a of the BWG, Article 98f, paragraph 4 of the VAG and Articles 6 and 12, paragraph 4 of the WAG; see also Chapter 3.6, crit. 13.1).

***Ex Parte Application for Provisional Measures (c. 3.3)***

221. Seizure and Sequestration are applied *ex-parte*, with an order by the office of the public prosecution or by the criminal police in the circumstances set out in Article 110, paragraph 3, in the case of seizure. Sequestration has to be requested to the court by the office of the public prosecution “immediately.” No prior notice is required.

***Identification and Tracing of Property subject to Confiscation (c. 3.4)***

222. It should be noted that Austrian criminal procedural law is based on the principle of legality, which makes it mandatory for law enforcement agencies to start an investigation if there is suspicion that a criminal offense has been committed (Article 34, paragraph 1, Article 36 and 99–100 of the StPO). This principle also applies to the identification and tracing of property that is subject to confiscation or suspected of being the proceeds of crime or used for FT. In such cases, the criminal police may take the necessary provisional measures (seizure) in order to secure the property, and prosecutors may make applications to the court for sequestration.

223. Credit and domestic financial institutions according to Article 1, paragraph 2 of the BWG (as well as DNFBPs) are required, upon request, to provide the A-FIU “with all information which the authority (that is the A-FIU) deems necessary in order to prevent or pursue cases of ML or FT” (e.g., Article 41, paragraph 2 of the BWG). In such case the A-FIU can request the information without the need of a court order.

224. However, this does not apply to other law enforcement agencies investigating ML or FT, or in those situations where the financial institution or DNFBP has refused to comply with the A-FIU’s request and the A-FIU must seek an order to compel the production of, or search persons and premises for, the documents. Up to now there was only one case known regarding the refusal of answering a request by the A-FIU, which was deferred by the reporting entity to the Independent Administrative Tribunal (*Unabhängiger Verwaltungssenat, UVS*). The UVS decided that the request by the BKA was legal and the information was subsequently transmitted to the BKA.

225. Specific provisions exist to empower the police and the A-FIU to access to information on bank accounts and bank operations. In such cases, for financial institutions, Article 116 of the StPO on “information on bank accounts and bank operations” will apply.

226. This provision requires that the disclosure of information on bank accounts and bank operation is admitted “if it seems necessary to ascertain a criminal offense or a misdemeanor under the jurisdiction of the regional courts (that includes ML) and sets the principle of “judicial admission”

for access to the information” (including for the search of the credit and domestic financial institutions according to Article 1, paragraph 2 of the BWG). This means that the office of the public prosecution must demand a court order and admission of the disclosure (or search).

227. The fact that in the above mentioned instances a court order is required to request (for law enforcement agencies) or to access/compel the information (for law enforcement agencies and the A-FIU) would not be an issue *per se*, except that the conditions for admitting the order are quite restrictive. The prosecutor must show on the basis of specific circumstances that the business relation of a person with the credit or financial institution is actually “connected to committing a criminal act” **and** that “either the holder of the account himself/herself is suspected of having committed the act or it is presumed that a person suspected of having committed the act will operate or has operated a transaction via the account”, **or** that “the business relation will be used for the transaction of a financial benefit that was gained through criminal acts or gained for them (Article 20 StGB) or is subject to the disposition of a criminal organization or terrorist group or is provided or collected as a means of financing terrorism (Article 20b StGB).

228. According to paragraph 4 of Article 116, the order and admission of the disclosure of information have to contain:

1. the denomination of the court case and the criminal act it is based on as well as its legal denomination,
2. the credit or financial institution,
3. the designation of the documents to be handed over and the information to be disclosed,
4. the facts that constitute the grounds for the necessity and proportionality (section 5) of the order,
5. in the case of an order according to paragraph 2 the time frame concerning which the operations are to be disclosed, and
6. in the case of an order, according to paragraph 2, the facts that constitute the grounds for the connection between the business relation and the subject of the proceeding.

229. Specifically, the court has to consider the issue of proportionality, that is, whether the disclosure and expected results are justifiably proportionate to the presumed infringement upon the rights of disinterested third parties and whether there could be also a reasonable chance of achieving the same result by taking less intrusive measures.

230. In the case of DNFBPs protected by professional privilege (lawyers and notaries) the conditions set forth in Article 9(4) RAO and 37(4) NO, discussed under the DNFBPs section, will apply. The very broad notion of “legal advice” (also discussed in that section) may substantially limit the right of law enforcement agencies to obtain information.

***Protection of Bona Fide Third Parties (c. 3.5)***

231. Specific provisions exist for the protection of *bona fide* third parties and, in any event, the State is ultimately responsible under the Public Liability Act for any decision taken by public authorities that violates private individuals' rights. Articles 20c and 26 of the StPO provide for abstention from forfeiture and confiscation if the property concerned is legitimately claimed by a person who has not participated in the offense or in the criminal organization or in the terrorist association (Article 20c) or for "objects" which are legitimately claimed by a person who has not participated in the offense, in which case they will only be confiscated if "the person concerned does not guarantee that the objects will not be used to commit the offense" (Article 26, paragraph 2). In the case of the A-FIU's power to freeze a transaction, the customer or "another party concerned" has the right to file a complaint with the Independent Administrative Tribunal or a complaint under Article 67 of the AVG.

***Power to Void Actions (c. 3.6)***

232. Adequate provisions exist also for voiding contracts that aim to frustrate claims resulting from the operation of AML/CFT laws.

233. Concerning the possibility of voiding contracts that aim to frustrate seizure, confiscation or forfeiture orders, the authorities pointed to Article 879 of the Civil Code (*Allgemeines Bürgerliches Gesetzbuch, ABGB*), which states as a general rule that contracts which violate existing (statutory) laws or which are *contra bonos mores* are null and void. This applies, for example, if the conclusion of the contract itself constitutes a criminal offense or if the contract was concluded with the intention to hinder the State's ability to recover legitimate financial claims. In addition to and irrespective of any such nullity, any act (like the conclusion of contracts or the transfer of assets) of a debtor that prevents any of his/her creditors from satisfying their legitimate claims may be contested under insolvency law and creditor's avoidance of transfers law.

***Additional Elements (Rec 3)—Provision for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture; and, c) Confiscation of Property which Reverses Burden of Proof (c. 3.7)***

234. The Austrian confiscation regime does not authorize civil (*in rem*) forfeiture, but provides for the forfeiture of property belonging to organizations that are found to be primarily criminal in nature (Article 20b of the StGB, in regard to property that is at the disposal of a criminal organization or a terrorist association).

235. Confiscation of such "membership benefits"—in principle—does not require a prior conviction for membership in a criminal organization or terrorist group, and the confiscation procedure is based on the partial reversal of the burden of proof in that the person subject to it has to show that the alleged benefits did not derive from his/her membership in a criminal organization or terrorist group. Legally, this provision operates on the basis of a legal presumption that any property within the possession of a person convicted to belong to a criminal organization or terrorist group does originate from such membership, but he/she can rebut it by making plausible to the court that his/her property came from a legitimate source.

**Effectiveness**

236. While the legal framework for the confiscation regime is robust in that it provides for a wide range of confiscation, seizure and provisional measures with regard to property laundered, proceeds from and instrumentalities used in and intended for use in ML and FT or other predicate offenses, and property of corresponding value, issues can be raised about its effectiveness.

237. Some of these issues stem from the restrictive conditions envisaged in certain instances, such as in the case of forfeiture of property at the disposal of the criminal organizations (for the difficulties to prove all elements constituting a criminal organization) or for the conditions for law enforcement to have access to information from financial institutions/DNFBPs (with the exception of A-FIU when investigating ML) or to compel documents held by these institutions. A particular concern is that, in practice, it seems that forfeiture of property at the disposal of the criminal organization or the terrorist group has not yet been applied (no specific figures were provided by the authorities in regard to this measure).

238. Although neither confiscation of profits or instrumentalities nor forfeiture require a criminal conviction, the authorities indicated that confiscation without conviction is rare in practice.

239. It is difficult also to ascertain the value of property which was subject to final confiscation in the statistics provided by the authorities (for the period 2004–2006), as the amounts indicated include also property subject provisional measures (which are not final measures). But even looking at these overall figures (which may be lower in reality if referred to confiscation only), there is a considerable gap when these amounts are compared to the statistics provided in regard to the interim injunctions applied by the A-FIU.

240. The following table shows the number of cases and the amount of property seized according to the former provision of Article 144a of the StPO (which provided for provisional measures), confiscated or forfeited according to Section 20 and Article 20b of the StGB during the time period 2003-2006 (no statistics are available for 2007).

Statistical Table 14. ML Offenses (Article 165 StGB)

	2003	2004	2005	2006
<b>Number of cases</b>	3	4	0	1
<b>Number of court orders (seizure/confiscation)</b>	3 (Article 144a StPO)	5 (Article 144a StPO)	0	1 (Article 144a StPO)
<b>Amounts of property seized/confiscated</b>	EUR 554.212,61 + USD 110.000	EUR 15.334.347	0	EUR 3.955.000

Statistical Table 15. Interim injunctions by court order applied for by the A-FIU

		2004	2005	2006	2007
<b>Injunctions (number)</b>		23	15	21	28
<b>Amounts involved</b>	<b>Accounts Deposits</b>	27.9	99.2	28	113.9

(EUR million)	Cash			0.2	
---------------	------	--	--	-----	--

### 2.3.2 Recommendations and Comments

241. The authorities should:

- Ease the requirements for law enforcement authorities to obtain access to information held by financial institutions and lawyers and notaries (for example, for financial institutions, permit wider access to such information for determining the nature of a criminal activity; permit the police to obtain such information with ex post judicial authority’s intervention, in the cases of serious crime; for lawyers and notaries revisiting the notion of “legal advice”);
- Consider the changes that need to be made in order to ease the burden in establishing that an organization is a “criminal organization” or otherwise change provisions so that Article 20b, when applied in the case of property at the disposal of such organizations, is more readily enforceable;
- Improve the effectiveness of the provisions by using them more frequently to restrain and confiscate criminal assets for ML, FT and predicate crimes, especially by making more use of forfeiture;
- Maintain more precise statistics on amounts restrained and confiscated in each instance.

### 2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	PC	<ul style="list-style-type: none"> <li>• Strict conditions for obtaining/compelling information subject to banking secrecy and scope of legal privilege hinder the possibility for law enforcement authorities to locate and trace property.</li> <li>• Given the level of profit-generating crimes, effective use of the provisional measures and confiscation provisions not demonstrated.</li> </ul>

## 2.4 Freezing of funds used for terrorist financing (SR.III)

### 2.4.1 Description and Analysis

#### Legal Framework

242. In Austria, measures to freeze funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance to the United Nations Security Council Resolutions (UNSCR) relating to the prevention and suppression of the financing of terrorist acts, are mainly implemented by means of directly applicable European Council Regulations (no. 881/2002 of May 27, 2002 and 2580/2001 of December 27, 2001, for UNSCRs 1267 and 1373, respectively). These Regulations are applicable for non EU-based entities or non EU residents or citizens listed as terrorists (hereinafter referred to as EU-externals). In addition to these Regulations, the EU adopted two Council Common Positions, No. 2001/930/CFSP and No. 2001/931/CFSP on the fight against

terrorism, which are applicable also to persons, groups and entities based or residents within the EU (hereinafter referred to as EU-internals), but their implementation required subsequent enactment of either binding EU Regulations or national legislation. The “Official Announcements” of the OeNB, issued pursuant to the DevG (Federal Law Gazette I No. 123/2003) serve this purpose, to a limited degree, in Austria.

243. The freezing power referred to therein are therefore exercised, depending on the persons concerned, either through this directly applicable EU legislation or, to a certain extent, through the above mentioned legally binding: “Official Announcements” of the OeNB. In addition and regardless the freezing obligation pursuant to the UNSCRs, if a founded suspicion arises that funds belong to terrorists or terrorist organizations, prosecutors also have a duty to institute criminal proceedings and apply for appropriate measures at court (provisional injunctions to freeze property, such as seizure or sequestration).

244. On September 3, 2008, the European Court of Justice issued a judgment in the *Kadi and Al Barakaat International Foundation* cases (C-402/05 P and C-415/05 P) that annulled the 2002 EU Council regulation that implements UNSCR 1267 and successor resolutions insofar as the regulation concerned the appellants. However, the Court in essence left the EU regulation in place for up to three months to permit the European Commission to remedy the violations found by the Court<sup>16</sup>.

245. The MoFA is the designated institution that collects and provides information to the UN Sanctions Committee on assets frozen in compliance with the relevant UN Resolutions.

246. Regarding the procedures for submitting national proposals in EU or UN-listing procedures, so far no proposal for a EU-or UN-listing has been put forward by Austria.

247. There are currently no funds frozen in Austria pursuant to UNSCRs 1267 and 1373 nor transactions were ever prohibited pursuant to the OeNB regulations based on Article 4 DevG. No violations of the freezing obligations have been recorded so far (therefore, no sanctions have been issued).

248. The 1267 list has currently one listing concerning a limited liability company formerly incorporated in Austria (*Youssef M. Nada & Co. Gesellschaft M.B.H.*). This company was dissolved on October 22, 2001, prior to the listing (which is dated November 2001) and subsequently deleted from the Commercial Register on November 14, 2003. The BVT reports that the accounts of the company were cleared before the listing took place in 2001, so no funds could be found after the listing.

249. There was only one case concerning the freezing of funds pursuant to UNSCR 1267. The account, on which USD 4,083.87 were deposited, had been inactive since February 19, 1987. On

---

<sup>16</sup> After the on site mission, in order to comply with the judgment of the Court of Justice, the European Commission adopted the Regulation (EC) no. 1190/2008 of November 28, 2008, amending Council Regulation (EC) no. 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with *Usama bin Laden*, the *Al-Qaeda* network and the *Taliban*.

March 4, 2002 the bank concerned supplied additional information reporting that the account holder died on January 3, 1987. Thus, the account was apparently frozen by mistake.

250. Finally, the authorities indicated that a freezing action in regard to a flat was undertaken pursuant to (EC Regulation 881/2001, therefore based on a 1267 listing) against a *Himmat Ali Ghaleb* (discussed later on).

***Freezing Assets under S/Res/1267 (c. III.1) and Freezing Assets under S/Res/1373 (c. III.2)***

251. Austria's framework for implementation of the financing of terrorism aspects of UNSCR 1267 and subsequent resolutions on the sanctions regime against *Al-Qaeda/Taliban* is through EC Regulation 881/2002. The implementation of UNSCR 1373 is through EC Regulation 2580/2001. These regulations are applicable in the case of EU externals only. For EU internals, the authorities consider that implementation of the relevant UNSCRs is through Official Announcement issued by the OeNB, pursuant to the Exchange of Control Act.

252. According to general European law principles, EU regulations are directly applicable in European national systems (EU member countries, as Austria), without the need of transposing these regulations into domestic legislation. As such, EC regulations 881/2001 and 2580/2001 serve as statutory law in Austria.

253. Under EC regulation 881/2001, all funds other financial assets and economic resources belonging to, or owned or held by a natural or legal person, group or entity designated by the Sanctions Committee and listed in the annex of the regulation shall be frozen. Annex I is regularly and promptly updated by the Commission every time a change is made to the UN list by the Sanctions Committee.<sup>17</sup>

254. The United Nations Security Council has indicated that the freezing orders be made within three working days after the date on which the UN determination has been made. A specific, accelerated procedure is followed to that end in the EU, which begins as soon as the European Commission is informed of a new determination and results in the publication of Regulations approved by the European Commission, which enter into force, with direct applicability across the EU, on the day of their publication. The European Commission does not give prior notice to the individuals and entities it designates, as this would undermine the effectiveness of the asset freezing. This has been upheld by the EU's Court of First Instance.

255. Regulation EC no. 2580/2001 (based on Common Positions 2001/930/CFSP and 2001/931/CFSP) established a freezing mechanism applicable against a designated list of persons/entities that are non EU-based entities or non EU residents or citizens ("EU externals"). Article 2 of this regulation contains the obligation to freeze funds, other financial assets and economic resources belonging to, or owned or held by, a natural or legal person, group or entity that is designated and listed (EU-externals), as well as the prohibition of making available to these persons/entities any funds, other financial assets and economic resources.

---

<sup>17</sup> The Commission is empowered to do so by Article 7 of Regulation (EC) no. 881/2002).

256. The list of persons, groups and entities to which this Regulation applies is established, reviewed and amended by decision of the Council, acting by unanimity. When determining if a person, group or entity should be targeted by freezing measures, the Council has to follow certain criteria stipulated in Articles 1(4), (5) and (6) of Common Position 2001/931/CFSP (Article 2). The Council decision is replaced every time the Council amends it. The current list of targeted persons can be found in Council Decision 2007/868/EC. The Council does not give prior notice to the persons it designates, as this would undermine the effectiveness of the asset freezing.

257. Financial institutions, other relevant institutions and authorities are required to directly implement Regulations 881/2001 and 2580/2001 by freezing the assets without delay of the designated persons and entities without prior notice. Upon freezing, financial institutions and others must notify the OeNB that they have frozen funds. In accordance with the EU regulations, OeNB is then to report this information to the Commission.

258. While the definition of “funds or other assets” contained in the EC Regulations is consistent with the same notion in SR.III, the direct applicability in Austria of these EU regulations presents some difficulties in regard to the freezing of other assets than funds held by financial institutions, such as real estate, businesses or undertakings, companies and vehicles. For these assets, in the Austrian legal framework, the freezing is practically applicable (and only to a limited extent) principally to the case of transactions that require registration (such in the case of immovable property, where the MoJ has issued instructions to the courts that maintain registers of immovable goods not to register transactions for goods that belong to listed individuals or companies). Therefore, the freezing measures as practically applicable in the Austrian framework are not in line with the broad terms envisaged by the interpretative note of SR.III, that define freeze as “prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism.” Moreover these freezing mechanisms do not allow a freezing “without delay” (in the sense required by SR.III).

259. The situation is particularly problematic for assets other than funds, as these assets may remain in the disposition of the listed persons, unless the act of disposition requires a transaction or contract that is subject to registration (and in Austria, in practice, this only applies to immovable goods, where specific MoJ decisions exist). In the case of immovable goods (such as real estate) the assessors were told that these goods are frozen only to the extent that any contract constituting rights on these assets which is subject to court registration will not be granted such registration (registration is a condition to transfer the right of property over an immovable good; the MoJ has issued specific instructions to the courts in this regard). For any other right that is not subject to court registration (such as a lease, for example), the authorities maintain that the contract will be considered null and void under Article 879 of the AGBG.

260. It has to be noted that in an Austrian court case concerning an immovable good owned by a person listed under EC Regulation 881/2002, the court established there is no obligation for the courts that maintain registers of immovable property to annotate on the register that the immovable good is subject to freezing under the relevant EU regulations. In the absence of an obligation to annotate the freezing (as it would be the case for provisional measures or for confiscation), the information on a good subject to freezing is seriously hindered.

261. Although, as in the case of immovable goods, the freezing would technically stem from the direct applicability of the EC Regulations it is not clear how the freezing obligation is implemented in practice in the case of other economic resources, such as companies or businesses and undertakings or vehicles held by listed persons. With regard to companies, the authorities indicated that when the sale of shares is subject to registration in the register of companies (as in the case of limited liability companies, for example) the register could deny such registration, by analogy with the registration of immovable goods in the relevant register. However, there is no case law or authority-issued instructions to confirm that this would be possible/required.

262. In regard to the implementation of UNSCR 1373 concerning persons, groups and entities based or residents within the European Union (EU-internals) which meet the criteria set forth by Article 1, c of the Resolution, these are excluded from the directly applicable requirements for the freezing of assets envisaged by the EC Regulation 2580, as noted earlier. These persons are listed in an Annex to the Common Position 2001/931/CFSP, which does not set directly applicable requirements in a EU country. This Common Position only requires EC countries to subject these persons to increased police and judicial cooperation between the Member States. Common Position 2001/930/CFSP, which also does not set directly applicable requirements in a EU country, requires EC countries to adopt freezing measures for funds and other financial assets or economic resources related to EU internals.

263. The authorities consider that the legal mechanism to address freezing obligations in the case of EU internals for the implementation of UNSCR 1373 in Austria is via Official Announcements of the OeNB setting regulations which can be issued pursuant to Article 3 of the DevG, in order to restrict capital movements under certain conditions, such as for complying with international legal obligations or for the protection of the legal interests of Austria.

264. The last regulation<sup>18</sup> was adopted by the OeNB on 25 September 2008 in order to incorporate Common Position 2007/871/CFSP into domestic law.

265. However, these regulations do not constitute freezing mechanisms in the terms required by UNSCR 1373 and SR.III as their scope is more limited. The requirements envisaged by the OeNB regulations are only applicable to the list of transactions described by Article 4 of the DevG these are transactions undertaken by or affecting rights of non residents, or involving foreign property owned by a resident or otherwise involving foreign means of payments, foreign currency or foreign securities.

266. While the banks met by the assessors were aware of the limitations set forth by the DevG for non-resident transactions they seemed not aware that the purpose of these provisions was the “freezing” terrorists’ assets. The nonbanking financial institutions met by the assessors seemed unaware of the existence of such “freezing” obligations.

### ***Freezing Actions Taken by Other Countries (c. III.3)***

---

<sup>18</sup> After the on-site mission the OeNB published on March 13, 2008 an updated version of the regulation (incorporating Common Position 2009/67/CFSP).

267. For the lists of persons and entities designated for freezing purposes through the EU regulations, Austria can freeze funds in accordance with UNSCRs 1267 and 1373 directly through the EU regulation mechanisms (with the limits described in the case of other assets than funds). For EU internals covered and designated by Common Position 2001/931 but not Regulation 2580/2001) Austria relies (with the limitations described earlier) on the Official Announcements issued by the OeNB.

268. For persons and entities who do not appear on any EU list, but for which Austria receives a direct freezing request from other jurisdictions, as well as circumstances where a freeze is necessary because of other information that indicates a possibility of financing of terrorism (e.g., information received through a STR), Austria has a judicial-based mechanism for seizure and confiscation of terrorist funds and, in addition, the power of the A-FIU to block an ongoing or postpone the execution of an imminent transaction reasonably suspected of serving ML or FT. Austria can also use, under the conditions and for the cases set forth in the DevG (described below) the freezing mechanisms envisaged by such law.

269. With respect to the obligation to act without delay, Austrian law provides for such actions to take place in exigent circumstances without a court order (in the case of seizure, which can be applied in first instance by the prosecutor or by the police). The authorities indicated that usually a request from a foreign authority to freeze assets, either with the mutual legal assistance channels or through the A-FIU can be taken swiftly (precedents were pointed out to the assessors). A 24-hour hot-line is established within the MoI for the adoption of urgent measures. However, since these are criminal procedure-related freezing, the prosecutor will need to have some evidence to substantiate the suspicions in order to maintain the assets frozen with a sequestration order by court. As noted earlier, confiscation or forfeiture is possible in principle without a conviction, but court-admissible evidence should be given to prove that property is at the disposal of a terrorist group or which has been provided or collected as a means of financing terrorism; also the court will have to establish a “terrorist group” offense, according to Article 278b (with the limitations illustrated in the case of the exemption provided by Article 278c, paragraph 3).

***Extension of c. III.1-III.3 to funds or assets controlled by designated persons (c. III.4)***

270. As previously mentioned, the assets subject to freezing are defined in very broad terms by the EU Regulations (for they include funds, other financial assets and economic resources); these assets are those “belonging to, or owned or held by” the designated persons/entities, “however acquired.” The language covers funds or other assets that are either directly or indirectly owned or controlled. While the EU Regulations are not explicit on the point of joint ownership, (rather implicitly recognizing that joint ownership is a form of ownership), the EU Best Practice of November 29, 2005 for the effective implementation of restrictive measures, which Austrian authorities are prepared to follow, provides that “funds and economic resources jointly owned by a designated person or entity and a non-designated one are in practice covered in their entirety. The nondesignated person or entity may subsequently request an authorization to use such funds and economic resources, which may include severing the joint ownership so that person’s share can be unfrozen.” More in general the Best Practice clarifies that “Holding or controlling should be construed as comprising all situations where, without having a title of ownership, a designated person or entity is able lawfully to dispose of or transfer funds or economic resources he, she or it does not own, without any need for prior approval by the legal owner.”

***Communication to the Financial Sector (c. III.5)***

271. The Council and the European Commission make their regulations and decisions public through the Official Journal of the European Union, which can be accessed by anyone on the website of the European Union. The authorities consider that publication in the official journal is sufficient notification to all for whom the legislation creates obligations and rights. For the same reason authorities consider that publication in the Official Gazette of the regulations of the OeNB and on its website constitutes sufficient notification to the financial sector. Some of the financial institutions which have correspondent relationships with the United States stated that they also receive the OFAC lists. These, as well as other lists, are supplied directly by external data providers.

272. The Austrian authorities indicated that they provide sanctions-related information to the relevant institutions. This dissemination also includes information on changes concerning foreign “national terrorist lists” for example, the OFAC list provided by the diplomatic representations of third countries forwarded to the MoFA or MoF. However, the financial institutions interviewed by the missions did not seem particularly clear to indicate which lists came or went or whose responsibility is was to send them.

***Guidance to Financial Institutions (c. III.6)***

273. With respect to communication and guidance, Austria relies in large part on the EU regulations itself to guide financial institutions and others, since the EU regulations have direct applicability to all EU entities and persons including those in Austria and there is a related obligation of Austria’s citizens and residents to know and act in accordance with the law.

274. The authorities indicated that the MoF, the OeNB or the WKO also provide detailed sanctions-related information either on individual request (by telephone or in writing) or due to recent developments of high importance. However, when meeting with the private sector, the assessors were

informed of difficulties is ascertaining the accuracy of false hits, in the absence of an official provider of information on the listed names.

275. In particular, although law enforcement officials check listed names against various databases, it does not appear there is a routine check of property ownership registers (for instance companies register) to determine whether a named individual or organization holds property in Austria and action taken to encumber property. The MoJ has issued guidance to the courts that maintain immovable goods registers not to grant registration to real estate transactions if one of the parties is in the EU lists.

***De-Listing Requests and Unfreezing Funds of De-Listed Persons (c. III.7)***

276. Relevant European regulations do not provide for a national autonomous decision regarding de-listing and unfreezing as a whole. Requests for de-listing have to be directed through the Federal Ministry for European and International Affairs (MoFA) and its representative in the relevant UN/EU body to the UN Sanctions Committee or the European Commission whichever is concerned.

277. Requests for de-listing from the list of persons and entities comprised by the UN sanctions against *Al-Qaeda* and the *Taliban* (the UN list) and the list of persons and entities comprised by the restrictive measures in EU Common Position 931/2001/CFSP (the EU list, which in Austria is implemented through Regulations) are to be directed to the OeNB as the designated competent authority.

278. Delisting matters may also be pursued before the Austrian and EU courts. In the case of refusal of a request of delisting, the applicant can decide to have the matter presented to a national Austrian court or to the European Court of Justice. If the challenge is to the legality of a designation under the regulations, the European Court of Justice can hear the complaint if made within two months after the designation. If the legality of a designation is lodged before a Austrian court, the court can present this question as a prejudicial question to the European Court of Justice.

279. Unfreezing in the case of mistaken identity may take place in the Austrian system in accordance with the EU Best Practices paper (“Effective Implementation of Financial Restrictive Measures targeting Terrorist Persons, Groups or Entities”), that is, a person may have his case considered by the OeNB which serves as the Austrian competent authority. The same procedure can be pursued following the AVG or by filing a case before an Austrian court.

280. Designations under the Regulations adopted by the OeNB pursuant to the Exchange of Control Act may be challenged under the AVG.

***Unfreezing Procedures of Funds of Persons Inadvertently Affected by Freezing Mechanism (c. III.8)***

281. The usual protections under Austrian law to the rights of *bona fide* third parties are applicable in the case of freezing under the EU lists or a seizure otherwise ordered in the Austrian system. Specifically, there is access to the courts in Austria to challenge aspects of a freeze that adversely affects a person or entity. The court could in turn seek the advice of the European Court of Justice. In addition, if the freeze is imposed through Regulation 881/2002 or 2580/2001, persons or entities may

institute proceedings before the European Court of Justice which is invested with authority to review the legality of such freezes. EC regulation 881/2002 at Article 6 also protects the good faith actions of freezing entities except when a freeze is due to negligence.

282. A person or entity who was erroneously listed by a regulation of the OeNB or a person whose funds were wrongly frozen by a financial institution may also seek damages in accordance with the Austrian law of damages and – where applicable – the Public Liability Act (*Amtshaftungsgesetz, AHG*).

***Access to frozen funds for expenses and other purposes (c. III.9)***

283. UNSCR 1267 as amended by UNSCR 1452 is implemented in the EU through a new Article 2a in EC Regulation 881/2002—directly applicable in Austria. This provision authorizes access to funds that are frozen for basic expenses, certain fees or for extraordinary expenses. The OeNB is the designated competent authority to receive requests from affected persons for exemptions. If so, the request is also notified to the *Al-Qaeda/Taliban* sanctions Committee which, within, 48 hours may object to the exemption. The OeNB must also promptly notify the person that made the request, and any other person, body or entity known to be directly concerned, in writing, whether the request has been granted or not. If the request is granted the OeNB has also to inform other Member States.

284. A procedure is also envisioned in Articles 5 and 6 of EC Regulation 2580/2001 which relates to designations emanating from UNSCR 1373. Under Article 5 the OeNB as the designated competent authority may grant a specific authorization to unfreeze funds for essential human needs under such conditions as it deems appropriate. Article 6 establishes a broader power for competent authorities of EU Member States to grant specific authorizations—with the view to protect the interest of the Community and the interest of its citizens and residents—after consultations with the other Member States, the Council and the Commission of the EU.

***Review of Freezing Decisions (c. III.10)***

285. As mentioned earlier, the freezing mechanisms envisaged by the relevant EC regulations can be challenged at the European Court of Justice by any natural or legal person that is directly and individually affected by it under the general principle established by Article 230 of the Treaty establishing the European Community. Under this general principle any natural or legal person may institute proceedings against a decision addressed to that person or against a decision which, although in the form of a regulation or a decision addressed to another person, is of direct and individual concern to the former.

286. A number of appeals against freezing orders based on Council Regulations (EC) no. 2580/2001 and 881/2002 are currently pending in the European Court of Justice. The appeals focus on claims that the human rights of the designated individuals, groups and entities were not respected. As regards Council Regulation (EC) no. 2580/2001, the Court of First Instance held in three judgments in 2006 and 2007 (T-228/02, *People's Mujahedin of Iran (OMPI)*, T-47/03, *Sison*, T-327/03, *Stichting Al Aqsa*) that the Council had to provide a statement of reasons to the designated individuals, groups and entities concerned, so as to allow them to make their views known on it and to allow the court to conduct a review. These judgments are final. The Court of First Instance upheld

this line of argument on 3 April 2008 in the cases T-229/02 and T-253/04, *Kurdistan Workers' Party (PKK)* and *Kongra-Gel*, which concern Council decisions made in 2002 and 2004.

287. On September 3, 2008, the European Court of Justice issued a judgment in the *Kadi* and *Al Barakaat International Foundation* cases (C-402/05 P and C-415/05 P) that annulled the 2002 EU Council regulation that implements UNSCR 1267 and successor resolutions insofar as the regulation concerned the appellants. However, the Court in essence left the EU regulation in place for up to three months to permit the European Commission to remedy the violations found by the Court. The Court found violations of fundamental human rights, specifically, the right of defense and the right to an effective legal remedy.

288. In cases where EU internals are designated by regulation of the OeNB the general principles of Austrian administrative law will apply, in particular Article 26 to 29 of the Administrative Court Act 1985 (*Verwaltungsgerichtshofgesetz, VwGG*).

***Freezing, Seizing and Confiscation in Other Circumstances (applying c. 3.1-3.4 and 3.6 in R.3, c. III.11)***

289. See analysis under paragraphs above.

***Protection of Rights of Third Parties (c. III.12)***

290. The rights of *bona fide* third parties affected by a freezing under the EU lists, OeNB designations or a seizure otherwise ordered in the Austrian system are protected by the relevant EC-Regulation as well as by the general principles of Austrian law.

291. If the freeze is imposed through Regulation 881/2002 or 2580/2001, the *bona fide* third party may institute proceedings before the European Court of Justice which is invested with authority to review the legality of such freezes. EC regulation 881/2002 at Article 6 also protects the good faith actions of freezing entities except when a freeze is due to negligence. There is access to the courts in Austria to challenge aspects of a freeze that adversely affects a person or entity: if the freeze (in the sense explained above) has been undertaken pursuant to the OeNB regulation the *bona fide* third party can also challenge it general principles of Austrian administrative law. Additionally, it also is a principle of the Austrian law of damages, that a person generally can only be held liable when it acted at least with negligence (see Article 1295 et seq. ABGB).

292. Finally, Articles 20c and 26, paragraph 2 StGB provide the legal basis for abstention from forfeiture and confiscation, if the property concerned is legitimately claimed by a person not having participated in the offense or in the criminal organization and are for this consistent with the standards provided in Article 8 of the Terrorist Financing Convention.

***Enforcing the Obligations under SR.III (c. III.13)***

293. Authorities are of the opinion that compliance with the relevant legislation is being generally monitored on a regular basis in the financial supervisory process, conducted by the FMA for the overall sector, the OeNB for the banks, and by external auditors, as part of their annual review. The authorities indicated that, the assessment of FT is an integrated part of the examination procedure of

the OeNB and that the examination methodology includes procedures to verify if the bank is in compliance with all provisions with respect to FT.

294. Assessors could not confirm that compliance to the obligations under SR.III are routinely monitored, and are of the view that further steps should be undertaken, especially in regard to the implementation of the DevG.

295. There is authority to impose sanctions for non compliance of the freezing obligations. The DevG stipulates that non-compliance with regulations of the European Community or relevant Austrian Federal Government Regulations concerning the freezing of funds is an offense punishable with a fine up to EUR 30,000 or a term of imprisonment of up to one year. Furthermore, the conclusion of a transaction which constitutes an offense of this Act is null and void. No sanctions have been issued so far for non compliance to this provision.

***Additional Element (SR.III)—Implementation of Measures in Best Practices Paper for SR.III (c. III.14)***

296. The authorities indicated that they have implemented the best practice paper for SR.III by way of the EU and domestic legislation described earlier in this section and that they fully cooperate with foreign jurisdictions.

***Additional Element (SR.III)—Implementation of Procedures to Access Frozen Funds (c. III.15)***

297. See discussion under criterion III.9

**2.4.2 Recommendations and Comments**

298. The authorities should:

- set up procedures within Austria that will ensure freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles);
- modify the OeNB regulations adopted pursuant to the DevG in order to make possible freezing of funds and assets held by EU-internals in all instances set forth by SR.III; and
- provide more guidance to the private sector, especially the non banking financial industry and DNFBPs, on the freezing obligations stemming from the international standard.

**2.4.3 Compliance with Special Recommendation III**

	Rating	Summary of factors underlying rating
SR.III	PC	<ul style="list-style-type: none"> <li>• Lack of effective procedures to allow freezing or to freeze without delay in the case of assets other than funds in many instances.</li> <li>• The OeNB regulations adopted pursuant to the DevG (for EU-internal terrorists) do not constitute freezing mechanisms in the terms required by UNSCR 1373 and SR.III, because they are mainly applicable to non residents and they do not encompass the full range of the economic</li> </ul>

		<p>resources.</p> <ul style="list-style-type: none"> <li>• Insufficient guidance provided to financial institutions and other persons or entities concerning their obligations under freezing mechanisms.</li> </ul>
--	--	--

## 2.5 The Financial Intelligence Unit and its Functions (R.26)

### 2.5.1 Description and Analysis

#### Legal Framework

299. The Austrian laws and regulations do not explicitly provide for the establishment of a Financial Intelligence Unit (FIU), but each of the ten laws and regulations covering the subjected entities refer to an authority that is competent for the reception of STRs in the case of ML or FT. The description of the competent authority varies for each reporting entity. The authority is the Federal Ministry of Interior for banks, insurance companies, investment companies, securities institutions, and most of the DNFBBs, with the exception of notaries and lawyers who have to report to the Federal office of criminal investigation (BKA), and accountants who have to report to the ML unit of the BKA. Despite these slight differences, the common understanding amongst the authorities and reporting entities, and actual practice, is that the STRs have to be reported to the Austrian Financial Investigation Unit (A-FIU) in the BKA. This is supported by the BKA website, the FMA circulars for financial institutions and the OENK guidance for notaries, and explanatory notes of some relevant laws. The A-FIU both receives all STRs and conducts criminal investigations on ML cases. The same law enforcement officers perform both tasks.

300. If information received by the A-FIU meets the requirements of an STR as defined in the laws, the A-FIU has to open an investigation. Pursuant to Article 1, paragraph 2 StPO “criminal proceedings start, as soon as police or public prosecution initiate investigations against a known or unknown person in order to clarify the suspicion of a criminal act.” The requirement to report a transaction when the financial institution suspects or has reasonable grounds to suspect that it serves the purpose of ML or FT falls into the scope of Article 1, paragraph 2 StPO. Consequently, the role of the A-FIU, regarding information it receives from reporting entities, is limited to establish that the information it receives qualifies as an STR. In 2007, out of the 1,085 information recorded as “STRs” in the A-FIU statistics, 197 cases were related to 419 letters or phishing emails, which did not meet the definition of an STR.

301. When the A-FIU receives STRs related to FT, it has to forward them to the BVT which is the competent authority for FT. As they both are law enforcement units, the A-FIU and the BVT need the opening of a case to exercise their powers (request of information from reporting entities, from other administrations, international cooperation, freezing of assets, special investigative techniques). Consequently, there is technically no dissemination of information by the A-FIU but investigations are conducted by the A-FIU or forwarded to another competent authority.

302. Pursuant to Article 49, paragraphs 1 and 3 StPO, the suspect/defendant has the right, to be informed about the nature of the suspicion raised against him (Article 50 StPO) and to have access to files (Articles 51-53 StPO). The right to access files also includes the right to inspect exhibits, as far

as this is possible without disadvantage for the investigation. Pursuant to Article 100, paragraph 3 StPO, the BKA report to the Prosecutor's Office shall include "the names of the persons who filed the criminal complaint, names of the victims and, if applicable, other informants." Under Austrian criminal law, when the preliminary proceedings ends or the case is final, the suspect/defendant is authorized to view all files related to the investigation (Article 194 StPO). This includes the STR with the name of the reporting entity. The right of the suspect/defendant to view all files related to the investigation can be restricted or certain data can be made anonymous, when there is danger for the personal security of an involved participant. But the right to access files may be limited only until the conclusion of the preliminary proceedings and is inadmissible if the suspect is in detention. (Article 51, paragraphs 2 and 3 StPO).

303. Following complaints by credit and domestic financial institutions, as their employees often felt exposed to potential threats or hostile action because they fear that their identity may become disclosed, a joint action plan by the authorities (MoF, A-FIU, MoJ, FMA, BVT and Federal Chancellery) and the financial sector (represented by the WKO) was agreed early November 2008. It contains measures to promote the protection of reporting entities and their employees (awareness raising campaigns both among the law enforcement authorities, public prosecutors, judges and the private sector; ordinances by the MoJ and the Federal Chancellery, anonymity of STRs, information on protective mechanisms contained in the StPO etc). Accordingly, a MoJ ordinance of November 11, 2008 gives guidelines regarding the protection of employees or reporting credit and domestic financial institutions.

***Establishment of FIU as National Centre (c. 26.1)***

304. In order to determine to what extent all the three core FIU-functions (reception, analysis and dissemination) are within the A-FIU's responsibility and how effectively they are implemented, it is worth analyzing in detail how these three functions are carried out in the Austrian system.

305. The obligation to report STRs is mentioned in each of the ten laws and regulations organizing the AML/CFT framework for the financial and non-financial institutions, but the authority competent to receive those STRs is slightly different depending on each law and regulation, as this appears in the following table.

Statistical Table 16. Reporting Entities

<b>Reporting entities</b>	<b>Legal basis</b>	<b>Competent authority</b>
Banks	Article 41 (1) BWG	Federal Ministry of Interior (Article 6 SPG)
Insurance undertakings	Article 98f(1) VAG	Federal Ministry of Interior (Article 6 SPG)
Investment Companies	Article 25 (5) BörseG	Federal Ministry of Interior (Article 6 SPG)
Securities institutions	Article 6 WAG	Federal Ministry of Interior (Article 6 SPG)
Casinos	Article 25a GSpG	Federal Ministry of Interior (Article 6 SPG)
Insurance Intermediaries, Real Estate Agents, Dealers, Management Consultants	365u(1) GewO	Federal Ministry of Interior (Article 6 SPG)

Lawyers	Article 8c, RAO	Federal Ministry of Interior (Federal Office of Criminal Investigation)
Notaries	Article 36c(1) NO	Federal Ministry of Interior (Federal Office of Criminal Investigation)
Accountants	Article 39(1) WT-ARL; Article 22(1) BiBu-ARL	The Money Laundering Centre at the Federal Office of Criminal Investigation

306. According to the laws, all financial institutions and most of the DNFBPs have to report to the authority under the Article 6 of the Security Police Act (*Sicherheitspolizeigesetz, SPG*) which is the MoI. It is constituted of the General headquarters for public security and the Federal Office of Criminal Investigation (BKA), the latter being organized according to a specific law, the BKA-G. Pursuant to Article 4(2) of the BKA-G, the BKA is competent to investigate ML in relation to the BWG, the BörseG and the WAG. The BKA-G entered into force in 2002, and as of that time only these laws contained ML and FT provisions. Concerning the FT, the BVT is the competent authority inside the Ministry of Interior. This is why, according to a letter from the BKA to the BVT, FT-related STRs are automatically forwarded to the BVT.

307. The organizational chart of the BKA shows a unit responsible for ML in the Department 3 (Investigations, Organized Crime and General Crime) which counts six sections, including one dedicated to Economic and Financial Investigations. One of its five units is the bureau 3.4.2, specialized on money laundering, also known as the A-FIU (Austrian Financial Investigation Unit). A similar unit was named EDOK until 2002, when the function of receiving STRs was absorbed by the BKA.

308. Despite the slight differences in the legal framework, it is commonly understood by the reporting entities that all STRs have to be sent to the A-FIU, and this appears to be the actual practice. This is supported by the BKA website, the FMA circulars for financial institutions, the OENK guidance for notaries, and explanatory notes of some of the relevant laws. Consequently, the A-FIU acts as a national center for receiving STRs and other reports concerning suspected ML, and STRs concerning FT activities. Suspicious transaction reports are usually transmitted by email, fax, post or courier to the A-FIU. The A-FIU also receives reports based on the suspicion of a violation of the obligation to disclose fiduciary relationships pursuant to Article 40, paragraph 2 of the BWG. It also receives reports related to withdrawal requests on savings deposit with a balance of at least EUR 15 000 when the identity of the customer has not being ascertained.<sup>19</sup> Based on Article 4(2) of the BKA-G, local police services are also required to inform the A-FIU about ongoing cases of ML. Finally, on the basis of the constitutional principle of cooperation between administrative authorities (Article 22 B-VG), the BKA is also the recipient of ML-related information from other administrations. There is no specific guidance or written directive regarding the application of this principle in relation to the work of the A-FIU, but the authorities consider that such guidance would be superfluous, as this principle is commonly understood and actual practice throughout the Austrian administration.

<sup>19</sup> Since November 1, 2000, customer identity has to be ascertained for savings accounts (including withdrawal and deposits on “old” savings accounts).

309. In 2007, the A-FIU received 2,247 information, including 1,599 reports from the professions subjected to reporting obligations. Out of those reports, 460 came from other law enforcement units, 514 were mandatory reports in relation to savings accounts and 1,085 were recorded as “STRs”, even if 197 cases were related to 419 letters or phishing emails, which did not meet the definition of an STR. The reports are received by an officer on duty in charge of the reception of the STRs. This function of officer on duty changes on a daily basis. Outside business hours, STRs are received by the SPOC (Single Point Of Contact) of the BKA.

310. With the exception of FT-related STRs from the reporting entities, the A-FIU is not responsible for receiving other FT-related information from other administrations, as the BVT is sole responsible for investigating FT. The distinction concerning the authority in charge of receiving information related to ML, on the one hand, and FT, on the other hand is evident in Article 17c (2) of the Customs Law (*Zollrechts-Durchführungsgesetz, ZollR-DG*), which, in connection with the performance of the control of cash brought in to/out of Austria, states that the customs authorities must pass the data to the competent authority, these being the A-FIU for ML and the Federal Agency for State Protection and Counter Terrorism (BVT) for FT, to the extent that this is necessary to perform their statutory tasks. In case the A-FIU receives FT-related information, it is forwarded to the BVT.

311. Concerning the analysis function of an FIU, the A-FIU being a law enforcement unit, it investigates complaints or STRs received under the scope of its competence and has to systematically start criminal proceedings in order to clarify the suspicion of a criminal act (Article 1, paragraph 2 of the StPO). Consequently, an investigation is open for each information received from a reporting entity when it meets the requirements of an STR (e.g., not one of the 419 letters or phishing emails). Consequently, the A-FIU has no analytical function. Indeed, a police investigation (Article 16 of the SPG) or a criminal investigation (Article 100 of the StPO) will be open based on the specificity of the report (e.g., a STR on a transaction that serves the purpose of ML or FT), and not on the evaluation of its utility or relevance.

312. As the A-FIU does not conduct analysis, it has also no dissemination function. After reception of information that meets the requirement of an STR, the first step is the opening of an investigation by the A-FIU and then the investigation is performed either by the BKA or the local police authorities for ML, and the BVT for FT, according to their respective responsibilities. As law enforcement authorities, they are all empowered to conduct investigative actions, such as surveillance, interrogations, wire-tapping, search of premises or issuing warrants of arrest.

313. Pursuant to Article 4(2) of the BKA-G, the BKA competence is “the fight against ML in relation to the BWG, BörseG and WAG”, and the BKA will consequently be in charge of investigations of ML-related STRs received on the basis of these laws. The circular allocating the functions inside the BKA makes clear that the A-FIU is the unit in charge concerning the information received by the BKA pursuant to section 41 of the BWG. The ML-related STRs based on the VAG, the GSpG and the GewO could theoretically be received and investigated by any police service, including, but not limited to, the BKA. Concerning the ML investigations that are on its single competence, the BKA is authorized to entrust local police services with investigations at any time.

314. As the BKA is not competent for FT, the cases regarding FT-related STRs are directly forwarded by the A-FIU to the BVT for investigation. This is made clear in the 16 June 2003 letter

10002/756-II/BK/3.42/03 from the BKA to the BVT which says that “Notification of suspicion of terrorist financing or of membership in a terrorist organization remains the direct responsibility of the BVT because of its original competence for such matters.” At the BVT’s request, the BKA can provide support to the investigation. The same circular requests the BVT to immediately inform the BKA (Money Laundering Notification Office, SPOC) if the grounds upon which an order has been issued cease to exist, as this is necessary in order to comply with the legal obligations for revoking an order.

315. The following table summarizes the responsibilities for receiving, analyzing and disseminating disclosures of STR and other relevant information concerning suspected ML or FT activities in Austria.

Statistical Table 17. FIU Functions

FIU Function	Competent Authority
Receiving STRs (ML/FT)	BKA (A-FIU) <sup>20</sup>
Receiving other relevant information – ML	BKA (A-FIU)
Receiving other relevant information – FT	BVT
Analyzing STRs and other relevant information	Not applicable
Disseminating STRs and other relevant information	Not applicable

***Guidelines to Financial Institutions on Reporting STR (c. 26.2)***

316. The A-FIU provides a specific reporting form for STRs which can be downloaded from the website of the Ministry of Interior ([www.bmi.gv.at](http://www.bmi.gv.at)). This website also includes information on the procedures that have to be followed when reporting. The reporting entities have to check a box on the STR form to indicate if the suspicion is based on ML or FT. Upon the reception of the STR, an investigation will be opened by the A-FIU and if the FT box has been checked, the case will be automatically forwarded to the BVT. This is recognized by both agencies as an extremely quick and efficient process that enables the BVT to be in a position to take adequate measures. The A-FIU can also be contacted by reporting entities in order to receive guidance regarding reporting on a case by case basis. During business hours, the contact is through the unit 3.4.2 (A-FIU) and outside office hours, the reporting entities can contact the SPOC of the BKA. The reporting entities clearly identify the A-FIU as the unit to be contacted in case of a need for guidance regarding the manner and procedures of reporting. The A-FIU estimates being contacted more than 10 times a day by reporting entities concerning their reporting requirements. The reporting entities met by the assessors are fully aware of this possibility.

<sup>20</sup> The BKA (A-FIU) is only a *de facto* competent authority for receiving all STRs, as the legal responsibilities are slightly different. Concerning ML, the BKA is legally competent for most STRs but not the one reported under the GewO, the GSpG and the VAG. Concerning FT, the BKA is not legally competent (except for accountants), but there is an agreement between the BKA and the BVT, so that the FT-related STRs are automatically forwarded to the BVT.

317. Additionally, the A-FIU provides information on reporting manners and procedures in informative meetings with reporting entities, either directly or organized by the reporting entities, the WKO, and the FMA.

***Access to Information on Timely Basis by the FIU (c. 26.3)***

318. Upon the reception of information by the A-FIU, no analytical function is performed on reports that meet the definition of a STR. A case is open and an investigation is started and conducted by the competent authority, either the BKA (including the A-FIU), the BVT or the local police with the powers set forth by the SPG and the StPO. FT investigations are always lead by the BVT itself or one of the LVTs. Local police authorities are consulted alternatively but they never lead FT investigations.

***Additional Information from Reporting Parties (c. 26.4)***

319. As investigations start immediately after the reception of STRs that meet legal requirements, all additional information is requested by the police authority in charge of the investigation, as part of the investigative process.

320. Once the investigation is open, the BKA is authorized to request directly all available and necessary information for ML and FT investigations from lawyers, notaries and accountants (see RAO, NO, WT-ARL and BiBu-ARL specify that it is the A-FIU) if released from the duty of secrecy by the client or if a judicial order is issued by the public prosecutor. Concerning casinos, gaming secrecy does not apply if released by the client or in the case of proceedings before civil courts and in connection with a criminal procedure subject to the StPO (Article 51 (2) GSpG). Concerning banks, insurance, investment and securities institutions, and other DNFBPs (see BWG, VAG, WAG, BörseG, and GewO), the relevant laws devolve the power to request information to the Federal Ministry of Interior, meaning that any department of the ministry, including the BVT is theoretically empowered to directly access financial information in the case of suspicion of ML or FT, based on its competence, without a court order. In practice, this power is exercised by the A-FIU. The authorities consider that the BVT would need a court order to request financial information from a reporting entity.

321. When related to a suspicion of ML or FT, the requested information is not subject to banking secrecy provisions. Persons and entities are obliged to provide the requested information to the relevant police authority. If the person or entity concerned refuses to provide information, sanctions may be imposed in accordance to Article 93, paragraph 2 StPO or a search warrant may be issued in accordance to Article 116, paragraph 6 StPO in order to enforce the obligation to disclose such information. Up to now there was only one case known regarding the refusal of answering a request, which was deferred by the reporting entity to the Independent Administrative Tribunal (*Unabhängiger Verwaltungssenat, UVS*). The UVS decided that the request by the BKA was legal and the information was subsequently transmitted to the BKA. In 2004 the BKA conducted 44 requests, 24 in 2005, 23 in 2006 and 105 in 2007, all towards banks. Even if police services other than the BKA could access financial information in case of a suspicion of ML or FT (except for lawyers, notaries and accountants), in practice all demands are centralized by the unit 3.4.2. of the BKA. As it is known as the A-FIU, it offers an identified point of contact for every financial and non-financial

profession. In practice, the A-FIU acts as a single point of contact for requesting additional information from the reporting entities during ML and FT investigations.

***Dissemination of Information (c. 26.5)***

322. As mentioned earlier there is no dissemination function, as the reception of an STR on a transaction that serves the purpose of ML or FT, amounts to the beginning of a police or judicial investigation. When the reporting entities indicate that the STR is related to FT, the report is immediately forwarded to the BVT. In other cases the A-FIU decides, depending on its competence and on territorial competence of the local police if it continues the investigation or forwards it to another unit in the BKA or to a local police authority.

Statistical Table 18. Authorities competent for investigating STRs

<b>Investigating STRs</b>	<b>Competent Authority</b>
ML-related suspected activities, in relation to the BWG, WAG, BörseG, GSpG	BKA (A-FIU)
Other ML-related suspected activities	Federal Police
FT-related suspected activities	BVT

323. It must be noted that each competent authority can request another police authority to provide support to the investigation. Following their investigations, the BKA, the Federal Police or the BVT have to systematically inform the Prosecutor's Office.

***Operational Independence (c. 26.6)***

324. The unit 3.4.2 (A-FIU) that receives STRs is part of the BKA, which in turn is subordinated to the MoI. The BKA has its own budget but there is no specific budget line for the staff and operations related to the reception of STRs.

325. Concerning the rules of nomination and the obligation to report, the A-FIU staff in charge of receiving and investigating STRs is subject to the general rules of the Austrian police. Inside unit 3.4.2, there is no distinction of responsibilities between staff in charge of the FIU function (receiving the STRs, including providing guidance to reporting parties) and staff in charge of the police or criminal investigations for money laundering. Indeed, each staff member performs tasks across the scope of competence of the unit 3.4.2.

***Protection of Information Held by the FIU (c. 26.7)***

326. The A-FIU maintains separate archives and its own file management, which access is protected. Only staff members of the A-FIU have access to the locked archives. The information received by the A-FIU is recorded in the general database of the BKA. But, access to information in this database is restricted and different access rights are provided. In general, except for the staff of the A-FIU, a positive request will be linked to a number and the information that a file is possessed by the A-FIU. But some of the high ranking officials of the BKA are provided with full access rights to the database.

327. Examples of STRs sent to the A-FIU that have leaked in the press or to suspected persons during an investigation have been mentioned by reporting entities. Reporting entities mentioned cases where the local police had disclosed an STR to suspected persons in order to justify an ongoing investigation. According to the authorities, information that leaked to the press were forwarded by the suspect's lawyers and other involved persons in the cases.

***Publication of Periodic Reports (c. 26.8)***

328. Since 2004 the A-FIU publishes annual reports that are presented in a press conference. These annual reports can be retrieved from the website of the MoI (<http://www.bmi.gv.at/publikationen/>). These reports describe detected and new trends and typologies, as well as information on the legal framework. They also include statistics regarding, among others, the number of STRs and breakdown by reporting entities, the number of anonymous savings account related reports, the cooperation with other countries, the predicate offenses concerning the STRs that are not related to self-laundering, the number of criminal charges for ML and the number of convictions. It should be noted that these reports are mainly oriented toward the ML-related activities and do not address explicitly FT.

329. The BVT has included a section on terrorism financing in its annual report, which is available on the website of the MoI. In the report for 2008, three pages were dedicated to FT, including an overview of trends and statistics.

***Membership of Egmont Group (c. 26.9)***

330. Austria is a founding member of the Egmont Group (1995) and regularly attends its meetings. It was first represented by EDOK and is represented by the A-FIU of the BKA since 2004.

***Egmont Principles of Exchange of Information among FIUs (c. 26.10)***

331. As a member of the Egmont Group, the A-FIU applies the Egmont Principles of Exchange of Information among FIUs which were adopted in The Hague on June 13, 2001. In 2007, the A-FIU sent/received information on 383 cases via the Egmont secure website. Additional information on international cooperation is provided under the analysis for R.40.

***Adequacy of Resources to FIU (c. 30.1)***

332. It is difficult to assess the adequacy of resources of the FIU functions of the Money Laundering Unit within the BKA because those functions are fully merged with the investigative functions. The latter is the main activity of the unit as the A-FIU is the only team dedicated to investigate ML in Austria. The staff of the A-FIU consists of the head, one secretary and three teams (total of 10 detectives<sup>21</sup>). The current resources concerning the investigation of ML cases have to be assessed regarding R.27.

---

<sup>21</sup> 11 detectives as of March 1, 2009.

333. In the absence of analysis, the reception of STRs is not the most costly function, especially in Austria where the level of STRs is relatively low, and there is no automated electronic transfer of data from the reporting entities. Reports may be sent by email but are not automatically integrated in the A-FIU database. The fact that the Money Laundering Unit performs both some FIU functions and investigations, put a constraint on resources and do not enable the unit to raise awareness on ML/FT typologies to reporting entities. Indeed, the staff of the A-FIU is in charge of the reception of STRs, ML investigations and some investigations on the predicate offenses.

***Integrity of FIU Authorities (c. 30.2)***

334. Regarding confidentiality, Article 20, paragraph 3 of the B-VG obliges all police officers and civil servants to professional secrecy. A breach of this principle can result in disciplinary measures, such as fines and dismissal. No specific provision applies concerning the dealing of information contained in STRs.

335. The current staffing of the Money Laundering Unit is made of law enforcement officers that have been trained to be detectives. They possess specialized knowledge to investigate white collar crime, mutual legal assistance, investigative methods, and computer handling. They are law enforcement officers, trained in search of premises, arrests, wire-tapping, international legal assistance and execution of letters rogatory, interrogations or surveillance methods. These appear to be appropriate skills to conduct police and criminal investigations.

***Training for FIU Staff (c. 30.3)***

336. It is possible for staff members of the Money Laundering Unit of the BKA to attend "refresher courses" regularly offered by the training agency of the police forces/MoI. The authorities consider that experience has shown that "training on the job" proves to be successful. Training courses can also be attended at the Vienna University of Economics and Business Administration. Additionally, the unit participates in international projects and seminars (Interpol, Europol, Egmont Group, Council of Europe, EUROJUST, FATF-Typologies workshops). Moreover, the unit participates actively in exchange programs with FIUs and law enforcement authorities in neighboring countries (Liechtenstein, Switzerland, Hungary and Slovakia). These training appear adequate and relevant for law enforcement officers.

***Statistics (applying R.32 to FIU)***

337. The Austrian authorities maintain comprehensive statistics on suspicious transactions reports and other reports, received and disseminated.

Statistical Table 19. STRs Received by the A-FIU<sup>22</sup>

	2004	2005	2006	2007
<b>ML-Related STRs</b>	373	467	692	1,085
<b>FT-Related STRs</b>	12	19	15	23
<b>Reports on Anonymous Savings Accounts</b>	1,206	1,009	1,174	514

338. The following tables show a breakdown by type of financial institution, DNFBP, or other business or person making STRs, for both ML and FT:

Statistical Table 20. ML-Related STRs

	2004	2005	2006	2007
<b>Financial institutions</b>	<b>360</b>	<b>426</b>	<b>658</b>	<b>1,045</b>
Banks	349	417	651	1,039
Insurance	11	9	7	6
Others (Stock exchange, Securities)	0	0	0	0
<b>DNFBPs</b>	<b>8</b>	<b>12</b>	<b>12</b>	<b>13</b>
Casinos	2	1	0	1
Lawyers	1	4	4	1
Notaries	2	3	2	3
Accountants	0	0	1	1
Real Estate Agents	0	1	0	1
Dealers	3	1	3	4
TCSPs	0	2	2	2
<b>Austrian administrations</b>	<b>5</b>	<b>29</b>	<b>12</b>	<b>27</b>
Ministry of Finance	0	27	7	21
FMA	5	2	5	5
Customs	0	0	0	1
<b>Total</b>	<b>373</b>	<b>467</b>	<b>692</b>	<b>1085</b>

339. It has to be noted that the statistics of the A-FIU envisage STRs in a broad sense as it also includes exchange of information from other administrations that are not STRs by the standard definition.

<sup>22</sup> The A-FIU considers every information received from a reporting entity as an STR, even if it does not meet the legal definition (131 information on “419 letters” and 66 phishing emails received in 2007 are included in the total number of STRs).

Statistical Table 21. FT-Related STRs

	2004	2005	2006	2007
Banks	9	16	14	20
Money transmitters	3	3	1	3
<b>Total</b>	<b>12</b>	<b>19</b>	<b>15</b>	<b>23</b>

340. Concerning statistics on the breakdown of STRs analyzed and disseminated, every STR on a transaction that serves the purpose of ML or FT is investigated.

***STRs resulting in investigation, prosecution or convictions for ML, FT or an underlying predicate offense (Additional element - c.32.3)***

341. Every STR on a transaction that serves the purpose of ML or FT has to be investigated by the A-FIU, the BVT, or the local police services. According to the StPO, every investigation case has to be submitted to the Prosecutor's Office.

342. It has to be mentioned that in the course of investigations, it is very often determined that the suspect is the primary offender ("self-launderer") and has to be charged for the "predicate offense", such as fraud, drug-related crimes, embezzlement, human trafficking, criminal organization, etc. In some STRs, the suspect turns out to be the victim of fraud, which leads to charges against real offenders. Cases submitted by the police to the prosecutor include therefore cases concerning the predicate offense itself. There is no information concerning the number of STRs resulting in convictions.

Statistical Table 22. Cases submitted to the Prosecutor

	2004	2005	2006	2007
<b>Cases Submitted to the prosecutor re. ML by the Austrian Police</b>	100	70	183	229
<b>Cases Submitted to the prosecutor by the A-FIU, not Limited to ML</b>	147	109	121	88

## 2.5.2 Recommendations and Comments

343. The authorities should:

- Review the legal framework in order to clearly establish a Financial Intelligence Unit that serves as a national center for receiving, analyzing and disseminating disclosures of STRs and other relevant information concerning suspected ML or FT activities;
- Empower this FIU to analyze STRs, prior to any police or criminal investigation, with access to the financial, administrative and law enforcement information and authorization to obtain additional information from reporting parties.

### 2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors underlying rating
R.26	PC	<ul style="list-style-type: none"> <li>• A-FIU not a national centre for analyzing and disseminating STRs.</li> <li>• A-FIU not a national centre for receiving, analyzing and disseminating information concerning suspected FT activities other than STRs.</li> </ul>

## 2.6 Law enforcement, prosecution and other competent authorities—the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R. 27 & 28)

### 2.6.1 Description and Analysis

#### Legal Framework

344. The legal framework is mainly constituted by the Criminal Code (StGB), the Code of Criminal Procedure (StPO) and by the Federal Act on the Organization of Security Administration and the Exercise of Security Police Services (Security Police Act, SPG, enacted in 1991 and amended in 2005).

345. Austrian law enforcement authorities have the responsibility and authority to ensure that ML and FT offenses are properly investigated. This responsibility is derived from Article 34, paragraph 1 of the StPO that requires that prosecutors prosecute *ex officio* all criminal acts which get to their knowledge and are not prosecuted only on demand of the victim or other interested parties (so called "*Offizialprinzip*"). ML and FT are therefore prosecuted mandatorily. This principle also implies that prosecutors must take all measures that are necessary to initiate criminal investigations. The Federal Criminal Police has general authority to conduct investigations on crimes and offenses set forth in the StGB, including for ML. In the case of ML the criminal investigations relating to the banking, investment and securities sectors are, *stricto sensu*, in the legal responsibility of the BKA where the A-FIU is located; in fact, pursuant to Article 4(2) of the BKA-G, the BKA is indicated as the competent authority to investigate ML in relation to the BWG, the BörseG and the WAG. However, according to the internal distribution of the workload within the BKA the A-FIU would be the authority in charge of ML investigations.

346. If financing of terrorism appears to be involved, the competent authority for criminal investigation is the Federal Agency for State Protection and Counter Terrorism (BVT).

#### *Designation of Authorities ML/FT Investigations (c. 27.1)*

347. The office of the public prosecutor has a general responsibility to prosecute all criminal acts, including ML and FT. This responsibility stems from the principle that requires prosecutors to prosecute *ex officio* all criminal acts which get to their knowledge. While the law does not specifically provide for the establishment of special sections in charge of financial crimes and organized crime within the public prosecutor's office, the larger public prosecutor's offices in the country have established groups of prosecutors who are only dealing with cases of organized crime and financial crimes (10 such prosecutors operate in Vienna).

348. For criminal investigations concerning ML and FT the responsibility is spread among the BKA, in which the A-FIU is established, the BVT and, ultimately, the Federal Criminal Police as a whole.

349. *Stricto sensu*, pursuant to Article 4, paragraph 2 of the BKA-G, the BKA has legal responsibility for criminal investigations of ML in relation to the BWG, the BörseG and the WAG, therefore with regard to the banking, securities and investment sectors. The A-FIU established within the BKA has the responsibility, nation-wide, to receive the STRs related to ML/FT that are filed by the whole range of reporting entities. The A-FIU also receives information on suspicious cases of ML that may come to the attention of other authorities (such as the Customs authorities). In these cases a criminal investigation is open. Criminal investigations on ML can then be undertaken by the A-FIU itself, “delegated” to local Federal Police (on the areas in which the BKA is legally responsible for investigating ML, mentioned above) or undertaken by the Local Federal Criminal Police territorially competent. If in STR or in the other ML-related information received, there are sufficient elements to indicate a particular predicate offense, the case is passed by the A-FIU to the competent law enforcement authority, either within the BKA itself or to the Federal Criminal Police. The BKA and the Federal Police report to the public prosecutor’s office.

350. The BKA is organized in 6 departments; department 3 (where the A-FIU is located) has the responsibility of investigations on “Organized Crime and general Crime.” There are 6 divisions in this Department: Organized Crime; Capital Crimes and sexual Offenses; Property Offenses; Economic and financial Investigations; Drug-Related Crime; and a central service for Combating Traffic in Human Beings and Illegal Immigration. The A-FIU is a sub-division of the Economic and Financial Investigations Division. Other subdivisions are responsible for fraud and counterfeiting; “white collar” crimes; environmental crimes; a subdivision is specifically dedicated to asset forfeiture (providing upon request assistance also to the financial investigators in the states’ headquarters of the federal Police). The A-FIU’s ML investigations are divided into three major areas: ML through the use of offshore; ML through frauds and ML related/associated to former Member States of the Union of Soviet Socialist Republics.

351. The BVT is a law enforcement authority, established within the MoI, Directorate General II for Public Security, legally responsible for investigation on cases related to FT, either originated from an STR (which is received by the A-FIU and forwarded to the BVT) or otherwise. Law enforcement authorities that come across a suspected case of FT must forward it to the BVT (this is the case, for example, when Customs authorities detect a suspicious cross-border transportation of cash which it is deemed to be related to FT, according to Article 17c, paragraph 2 of the Customs Code). The BVT has also 9 regional departments and reports to the public prosecutor’s office.

***Ability to Postpone / Waive Arrest of Suspects or Seizure of Property (c. 27.2)***

352. According to Article 99, paragraph 4 of the StPO the police has the authority to postpone investigations and the adoption of coercive measures if:

- this was conducive to the clarification of a more grave offense or the investigation of a leading person in the offense and the postponement caused no serious danger for life, health, physical inviolability or the freedom of third people; or

- otherwise a serious danger for life, health, physical inviolability or the freedom of a person was caused.

***Additional Element—Ability to Use Special Investigative Techniques (c. 27.3)***

353. The following special investigative techniques are permitted by the StPO or the SPG:

- Observation (defined as “secret surveillance of the conduct of a person, regulated by Article 130 of the StPO and admissible for criminal acts);
- undercover investigation (defined as “the use of officers of the criminal police or other persons on order of the criminal police, who do not disclose nor show their official position of their tasks, regulated by Article 131 of the StPO and admissible if it appears necessary to clarify a criminal act);
- Fictitious purchase (defined as “the attempt or the feigned committing of a criminal act as far as this consist in the acquirement, purchase, possession, export, import or transport of objects or assets that have been alienated, originate from a crime or are dedicated to committing a crime or the possession of which is absolutely prohibited” regulated by Article 132 StPO and admissible only for crimes, therefore not for ML); and
- monitoring of data, interception of telecommunications, audio-visual monitoring of individuals by technical means and computer-aided data cross-referencing (Articles 134-143 StPO).

354. These techniques can be undertaken by the Criminal Police at their discretion or with the authorization of the public prosecutor’s office.

***Additional Element—Use of Special Investigative Techniques for ML/FT Techniques (c. 27.4)***

355. Special investigative techniques are mostly used in investigations into organized crime and terrorist crimes. The A-FIU pointed out the frequent use of interception of communications and surveillance of target persons during its investigations of ML cases.

***Additional Element—Specialized Investigation Groups & Conducting Multi-National Cooperative Investigations (c. 27.5)***

356. While the law does not specifically provide for the establishment of special sections in charge of financial crimes and organized crime within the public prosecutor’s office, the larger public prosecutor’s offices in the country have established groups of prosecutors who are only dealing with cases of organized crime and financial crimes. The authorities estimate that out of 300 prosecutors operating in Austria approximately 10 percent is specialized in ML and financial crime investigations. The BKA has a specialized division in charge of economic and financial investigation, in the context of which A-FIU is located as well as a division specifically in charge of tracing proceeds of crime for assets forfeiture. The BVT uses regularly financial investigations with the purpose of understanding the structure of the terrorist groups.

357. Cooperation in investigation, including in the use of special investigative techniques, is possible, at EU level, within joint investigative teams among law enforcement authorities of EU Member States.

***Additional Elements—Review of ML & FT Trends by Law Enforcement Authorities (c. 27.6)***

358. Regular information exchange takes place between relevant staff of the MoJ, Public Prosecutor's Office, courts and the MoI (A-FIU and BVT). There are also regular meetings with the authorities involved in supervision and/or AML/CFT policy for financial institutions (MoF, OeNB, FMA).

***Ability to Compel Production of and Searches for Documents and Information (c. 28.1)***

359. According to the authorities, the A-FIU is the only law enforcement agency entitled to request directly all available and necessary information from persons and entities subject to reporting obligations without the need of a court order. But concerning banks, insurance, investment and securities institutions, and other DNFBPs (see BWG, VAG, WAG, BörseG, GSpG and GewO), this power is devolved to the MoI, meaning that the BVT is theoretically empowered to access directly financial information in the case of suspicion of FT without a court order.

360. Person and entities are obliged to disclose information to the A-FIU, as the information requested in the case of suspected ML/FT is not subject to banking/professional secrecy provisions.

361. Other law enforcement agencies investigating ML or FT, and the A-FIU need a court order when they have to compel the production of or search persons and premises for documents held by financial institutions/persons (with a “judicial admission” procedure, discussed later on).

362. Law enforcement agencies other than the A-FIU must be authorized with judicial admission in the circumstances set forth by Article 116 of the StPO to request information on bank accounts and bank operations. This provision requires that the disclosure of information on bank accounts and bank operation is admitted “if it seems necessary to ascertain a criminal offense or a misdemeanor under the jurisdiction of the regional courts (that includes ML) and sets the principle of “judicial admission” for access to the information, which means that the office of the public prosecution must demand a court order and admission of the disclosure.

363. The conditions for admitting the order are quite restrictive. The prosecutor must show on the basis of other evidence (“ascertained facts”) that the business relation of a person with the credit or financial institution is actually “connected to committing a criminal act” **and** that “either the holder of the account himself/herself is suspected of having committed the act or it is presumed that a person suspected of having committed the act will operate or has operated a transaction via the account”, **or** that “the business relation will be used for the transaction of a financial benefit that was gained through criminal acts or gained for them (Article 20 StGB) or is subject to the disposition of a criminal organization or terrorist group or is provided or collected as a means of financing terrorism (Article 20b StGB).

364. According to paragraph 4 of Article 116, the order and admission of the disclosure of information have to contain:

1. the denomination of the court case and the criminal act it is based on as well as its legal denomination,
2. the credit or financial institution,

3. the designation of the documents to be handed over and the information to be disclosed,
4. the facts that constitute the grounds for the necessity and proportionality (section 5) of the order,
5. in the case of an order according to paragraph 2 the time frame concerning which the operations are to be disclosed, and
6. in the case of an order according to paragraph 2, the facts that constitute the grounds for the connection between the business relation and the subject of the proceeding.

365. Specifically, the court has to consider the issue of proportionality, that is,, whether the disclosure and expected results are justifiably proportionate to the presumed infringement upon the rights of disinterested third parties and whether there could be also a reasonable chance of achieving the same result by taking less intrusive measures.

366. In the case of DNFBPs protected by professional privilege (lawyers and notaries), the conditions set forth in Article 9(4) RAO and 37(4) NO), discussed under the DNFBPs section, will apply. The very broad notion of “legal advice” (also discussed in that section) may substantially limit the right of law enforcement agencies to obtain information.

367. The search of credit and domestic financial institutions according to Article 1, paragraph 2 of the BWG (as well as the search on persons that are protected by professional secrecy, and the search of their premises) always requires a judicial admission.

368. Seizure and sequestration of documents (including transactions records, identification data obtained through the CDD process, account files) can be obtained under the circumstances set forth by Articles 110 and 115 of the StPO: therefore only if these objects required for evidentiary purposes, or for securing civil right claims, confiscation of profits (Article 20 of the StGB), forfeiture (Article 20b of the StGB), confiscation (Article 26 of the StGB) or any other order relating to property rights provided for in the law. They are not admitted if the purpose is only ascertaining the commitment of a crime. They are ordered by the public prosecutor’s office or by the court. Sequestration of business correspondence falls under the circumstances set forth by these two provisions, unless in the case of closed correspondence that has not yet reached the recipient, in which case the more restrictive conditions established by Article 135 (sequestration of letters, which regulates the case of opening and retaining the telegrams, letters or other mail sent by or destined for “the accused”, which is only admissible for clarifying an intentional criminal act punished with a prison sentence exceeding one year and if the accused is imprisoned for such an act or if his production or arrest has been ordered regarding that act) would apply.

***Power to Take Witnesses’ Statement (c. 28.2)***

369. The competent authorities (office of the public prosecutor and the courts) have the powers to take witnesses’ statements for use in investigations and prosecutions (Articles 151–166 StPO). These provisions apply generally and are also available in ML or FT investigations and prosecutions.

370. Measures to protect witnesses which may be at risk in the circumstances of a criminal procedure include provisions to hear witnesses without their identity being disclosed, allowing pre-trial records of cross-examination of witnesses, conducting questioning by means of telecasting if a witness is unable to appear in court without exposing him/herself to a serious threat and conducting closed court hearings. The application of such measures is decided by the public prosecutor and/or the court (Articles 161 and 165 StPO).

***Adequacy of Resources to Law Enforcement and Other AML/CFT Investigative or Prosecutorial Agencies (c. 30.1) and Integrity of Competent Authorities (c. 30.2)***

**Prosecutorial Agencies**

371. The offices of public prosecution are autonomous agencies of the judicial administration which are separate from the courts. They safeguard the interests of the state in the adjudication of law. Among their most important tasks is to lead the preliminary investigation and to represent the public prosecution in penal proceedings. The Public Prosecution Act governs these tasks. In contrast to judges, public prosecutors are bound by the instructions of their superiors. Instructions from higher authorities concerning actions in a specific proceeding must be justified and issued to the public prosecutors in writing and becomes part of the file. At first-instance courts their responsibilities are vested in the public prosecutor, at the court of appeal in the senior public prosecutor and at the Supreme Court in the general procurator. The offices of senior public prosecutors and the General Procurator's Office are each only subordinate to the MoJ. A general procurator does not have any authority to issue instructions to senior public prosecutors or public prosecutors. At present, there are about 300 public prosecutors in Austria.

372. Only judges or former judges, who continue to meet the requirements for being appointed as professional judges, may become public prosecutors. Just as the established posts for judges, the established posts for public prosecutors are also advertised publicly to applicants. The Federal President appoints public prosecutors upon proposal by the staff commission. However, for most established public prosecutor posts the President has delegated the right of appointment to the Federal Minister of Justice.

373. If a public prosecutor is found guilty of violating the professional and ethical obligations, he/she is responsible to a disciplinary commission set up with the MoJ. The sanctions which this commission may impose also include termination of the employment relationship. In addition, public prosecutors also have a penal-law liability. In terms of civil law, public prosecutors may only be held responsible by the state, similarly to judges, and not by the parties involved in a case, who may only bring an action against the state for official liability.

**Criminal Police**

374. As of December 1, 2008, the Police has a current staff of 26,984 policemen and 5,407 administrative staff. A recent report of the Audit Agency stated that the Police may not be staffed enough, a view which is shared by the Police. The Police is otherwise adequately structured and funded, and provided with sufficient and technical and other resources to fully perform their functions. Staff is required to maintain high professional standards, including confidentiality.

**BVT**

375. The number of officials working for the BVT could not be disclosed to the assessors for reasons of confidentiality; however the officials met by the assessors stated that the number of officials employed is sufficient, and that the agency is adequately funded, and provided with sufficient technical and other resources to fulfill its functions.

***Training for Competent Authorities (c. 30.3)***

376. Training is provided to administrative, investigative, prosecutorial, and judicial authorities. Training is provided to the judicial authorities in the frame of the annual further training program, organized by the MoJ. Especially concerning the topics ML and FT there have been held several training programs (authorities indicated that two to three seminars are organized every year by the MoJ concerning financial crimes); some of them in cooperation with other institutions, such as the MoI. Judges and public prosecutors are offered to partake in those trainings. An extensive training specifically on ML and FT was last organized in 2006 (*Ottenstein*). This one-week training course was attended by about 55 judges and public prosecutors.

377. Since 1998, the MoJ also encourages judges and public prosecutors to participate in international trainings dealing with combating ML and FT. A number of judges and public prosecutors attended those trainings (e.g., the conferences of EUROJUST on terrorism in 2004 and 2005 in The Hague).

378. The training department of the BKA organizes special training courses in regular intervals for police services on ML but also on predicate offenses such as human trafficking, narcotics trafficking, etc. The A-FIU is very active in providing training for the private sector as well as for other authorities. Upon request of local police services, specific training seminars are held by the A-FIU. The total number of training and awareness raising seminars offered to various target groups is listed in the A-FIU's annual reports.

379. BVT employees working in the CFT area have access to further training opportunities on the national and international level. BVT aims at participating in as many international trainings and workshops as possible. In this context, the workshops organized by EUROPOL, Interpol, foreign partners, such as for example, the training courses of the German Federal Criminal Police Office and those organized by the intelligence can be mentioned.

380. The acquired experiences and information are then spread on by BVT to the LVTs in the framework of regular meetings, to ensure that also the investigators in the federal states are permanently provided with up-to-date knowledge and information.

***Additional Element (Rec 30) - Special Training for Judges (c. 30.4)***

381. See reference to training for judges under criterion 30.3.

**2.6.2 Recommendations and Comments**

382. The authorities should soften the requirements for law enforcement authorities to obtain access to information held by financial institutions and by lawyers and notaries (for example, for

financial institutions by envisaging also the access to such information for the purpose of ascertaining a crime or by allowing the police to obtain such information with ex post judicial authority's intervention, in the cases of serious crime; for lawyers and notaries by revisiting the notion of "legal advice").

### 2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors underlying rating
R.27	C	
R.28	LC	Strict conditions for obtaining/compelling information subject to secrecy and scope of legal privilege hinder the possibility for law enforcement authorities to locate and trace property.

## 2.7 Cross Border Declaration or Disclosure (SR.IX)

### 2.7.1 Description and Analysis<sup>23</sup>

#### Legal Framework

383. Austria applies EC Regulation 1889/2005 on controls of cash entering or leaving the community (EC cash control regulation) to cross-border transportation of currency and bearer negotiable instruments at its borders with non-EU countries, that is, Switzerland and Liechtenstein. The EC Regulation is directly applicable in Austria as an EU member. For EU-internal borders (i.e., borders with Germany, Hungary, Italy and Slovakia) Austria applies the Customs Law (ZollR-DG), with the notable exception of the borders with Jungholz and Mittelberg: both Jungholz and Mittelberg are Austrian enclaves in the territory of Germany which have been historically exempted from the application of the Austria ZollR-DG and which, as the authorities explained, are subject to German customs law, by international treaty.

384. The EC Regulation establishes an obligation to declare cash of a value of EUR 10,000 or more when entering or leaving the EU space. The ZollR-DG subjects to customs supervision cash and cash-equivalent means of payments which are brought in the "area of application" of the law (that is Austria with the exception of the above mentioned enclaves). In this case the ZollR-DG establishes an obligation to disclose upon request of the Customs authorities cash or equivalent of a value of EUR 10,000 or more. This obligation was introduced in 2004 and 2006.

#### *Mechanisms to Monitor Cross-border Physical Transportation of Currency (c. IX.1)*

<sup>23</sup> The FATF agreed to the revised text of the Methodology criteria on SR IX to address issues relating to the application of SR.IX to supranational jurisdictions in February 2009. As indicated during the February 2009 Plenary Meeting of the FATF, Austrian authorities could have chosen to be evaluated on the revised standards. However, the authorities and the assessor team agreed that the assessment will refer the Methodology re SR.IX as of the date of the submission of the Detailed Assessment Questionnaire, considering that papers providing guidance for assessment and developing further best practices on SR.IX in the supra-national context are not available yet, and could not be considered in the assessment of SR.IX under the revised Methodology.

385. Austria relies on a declaration system for cross-border transportation of cash of a value of EUR 10,000 or more at its non-EU borders. The obligation is established by Article 3 of EC Regulation No. 1889/2005 and is consistent with SR.IX. Article 2 defines cash as including currency and bearer negotiable instruments including monetary instruments in bearer form (such as travelers cheques), negotiable instruments that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such a form that title thereto passes upon delivery as well as incomplete instruments (such as promissory notes and money orders) signed but with the payee's name omitted. In this case, Article 17b, paragraph 3 of the ZollR-DG clarifies that the declaration must be rendered verbally but the declaring person has also the option to submit the declaration in written form.

386. In addition to the declaration system, Article 17b of the ZollR-DG, paragraph 1, subjects to customs supervision cash and cash-equivalent means of payments which are brought "into, through or out the area of application" of the ZollR-DG, and (paragraph 2) establishes an obligation to disclose upon request of the Customs authorities cash or cash-equivalent means of payments of a value of EUR 10,000 or more. "Cash-equivalent means of payments" are defined (by paragraph 1 of Article 17b) in the same terms as in the EU Regulation but, in addition, they also include "gold and other precious metals." The disclosure system is applicable for the cross-border transportation of cash and other bearer negotiable instruments at the EU-borders, with the noted exceptions of Jungholz and Mittelberg, where no obligation to declare or to disclose exists in the terms required by SR.IX. This can pose a risk of ML and FT, given the number of bank accounts existing in these areas, which is significantly disproportionate to the number of residents (the issue is discussed later in more details).

387. The authorities explained that in order to detect cash couriers they employ a risk-based approach at Vienna airport (in the case of incoming/outgoing flights to areas considered at risk) or random checks; they employ a targeted risk-based approach at the borders, but only as part of anti-smuggling operations (especially for cigarette-smuggling).

Statistical Table 23. Statistics Cash Control Austria

	<b>15.06.2007- 30.09.2007</b>	<b>01.10.2007- 31.12.2007</b>	<b>01.01.2008- 31.03.2008</b>	<b>01.04.2008- 30.06.2008</b>
Declarations	494	461	627	645
Total Sum (EUR)		918,301,298	1,155,292,204.5 8	810,960,980
Oral Declarations	3	5	7	1
Written Declarations	491	456	620	644
Declaration by Private Persons		82	100	99
Sum (Private Persons) (EUR)		8,667,324	12,374,909.88	9,433,504.25
Declaration by Cash Couriers		379	520	546
Sum (Cash Couriers) (EUR)		909,633,974	1,142,917,294.7 0	801,527,475
Non Declared	0	2	7	1
Sum (Non Declared) (EUR)		659,219	453,686	26,500
Export to US	2	3	5	0

Sum	USD 99,107	EUR 121,539	EUR 392,715	0
Import from US	1	2	1	3
Sum	USD 18,385	EUR 78,325	EUR 31,683	45311
Export DE -to CH	10	11	49	65
Sum DE - CH	287,803.6	686,360	87,866,861	90,894,877

***Request Information on Origin and Use of Currency (c. IX.2)***

388. Article 17b of the ZollR-DG – which is applicable in all cases of cross-border transportation of cash, regardless the “type” of border – establishes a general obligation to provide, upon request of the Customs authorities, “information on the origin, the beneficiary and the intended use of the cash.” This obligation sets a general authority for Customs officials to request such information in the case set forth by paragraph 2 (which sets forth the “disclosure” obligation) and, as the authorities explained, also in the case of “declarations” (which are regulated by paragraph 3 of Article 17b) including in the case of a false declaration or in the case of a failure to declare.

***Restraint of Currency (c. IX.3)***

389. Article 17c of the ZollR-DG states that when “certain facts give rise to the assumption that cash or equivalent means of payment are introduced for the purpose of ML or FT, the Customs authorities are authorized in case of danger to seize the cash or means of payments.” In such cases, the Customs authority has to report immediately to the public prosecutor’s office, which has to determine whether the conditions sets forth by Article 115 of the StPO are met to apply a sequestration (discussed earlier). If they are not met the seizure has to be terminated without delay. Otherwise the provisional measure remains in place for up to six months (unless the court orders the seizure to be terminated). There are no statistics available on the cases/amounts of seizure of cash, but it looks like the provisional measure has been rarely applied. The authorities indicated a recent case in which USD 600,000 were found in the luggage of an individual and seized on the grounds of ML, but the seizure was dismissed by the public prosecutor’s office.

***Retention of Information of Currency and Identification Data by Authorities when appropriate (c. IX.4)***

390. Customs authorities have legal authority to collect, process and use the personal data gathered from the declaration/disclosure requirements (Article 17c, paragraph 2 ZollR-DG). However there is no central database where all the data gathered through this process is stored or can be queried. All declarations are stored in hard copies at the customs offices to which the declarations were made. The data collected are summed up and reported quarterly in electronic form to the MoF (who forwards this information to the EC), but these data only regard the number of declarations broken down per border points where the declaration was made, with the overall amount of money involved. Currently no analysis is carried out on these data for developing intelligence for AML/CFT, nor is it possible to target a person as cash courier based on how frequently he/she had declared/disclosed. The authorities are planning to set up a computerized database with the view of using the information collected under the declaration/disclosure process for building up intelligence for AML/CFT.

***Access of Information to FIU (c. IX.5)***

391. Although there is an obligation for the Customs authorities to pass the data gathered from or otherwise relevant to the A-FIU and the BVT “to the extent that this is necessary to perform their statutory tasks” (Article 17c, paragraph 2 ZollR-DG) this information is not currently made available to the A-FIU, except when Customs suspect ML. Austria therefore implements a system whereby the A-FIU is notified about suspicious cross border transportation incidents that gives rise to a suspicion of ML or FT: this has occurred only once in 2007 and five times in 2008 (for ML only). In the case of suspicions of FT, the information is passed on to the BVT. No cases were reported to the BVT.

***Domestic Cooperation between Customs, Immigration and Related Authorities (c. IX.6)***

392. Although a coordination mechanism is not formally established, Customs authorities undertake regular meetings between the MoF (Division for Enforcement of Taxes and Customs) and the BKA to discuss and coordinate on matters of common interests or linked to tax or customs fraud and organized crime. Additionally, informal information exchange takes place on a case-by case basis in urgent matters. The Customs authorities have access, through the investigation branch of the Customs Office, to the contact point within the MoI and to the criminal record database.

***International Cooperation between Competent Authorities relating to Cross-border Physical Transportation of Currency (c. IX.7)***

393. Articles 6 &7 of EC Regulation No. 1889/2005 set the basis for the exchange of information with third countries. Article 6 is applicable for the exchange of information between EU member States, and it states that when there are indications that the sums of cash are related to any illegal activities associated with the movement of cash and in the case of ML the information gathered through the declaration process may be transmitted to competent authorities in other member states. Article 7 deals with exchange of information with non EU member States upon certain conditions. As a member of the EU Austria also applies the EC Regulation 515/97 on mutual assistance in customs matters applies.

394. Austrian Customs have signed bilateral agreements for cooperation with 20 countries within the EU and with 50 countries outside the EU. These agreements require ratification by parliament (which occurred in all these cases).

395. Austrian Customs take part in the EC-Cash Control Committee. The points discussed include exchange of information about best practices on procedures and use of declaration forms as well as the discussion of concrete cases and lessons learned.

***Sanctions for Making False Declarations / Disclosures (applying c. 17.1-17.4 in R.17, c. IX.8)***

396. Sanctions for non compliance with the obligations to declare or to truthfully disclose set forth by the ZollR-DG are laid down in Article 48b of the Fiscal Penal Code (*Finanzstrafgesetz, FinStrG*). The penalty is up to EUR 50,000 (intent) or up to EUR 5,000 (negligence) and is in compliance with the requirements set forth by Recommendation 17. The sanction is a criminal sanction applied by the Customs authorities in the context of an administrative penal procedure.

397. The authorities indicated that six offenses were committed by intent and two by negligence in 2008; in all cases monetary fines have been imposed, though it was not possible to have concrete information on the amount of these fines as this information is not maintained in the Fiscal Penal Register (which does not contain data on the concrete cases).

398. The sanctions are also applicable in the case of legal persons (Article 28a FinStrG in connection with provisions of the VbVG) if :

- the duty to declare information refers to the legal person or;
- the infringement of this duty was done in favor of the legal person; and
- either the person with a leading position (decision maker) or other persons of the management themselves failed to declare or disclose the relevant information or they did not take care to ensure that this duty was complied with by the employees of the legal person.

***Sanctions for Cross-border Physical Transportation of Currency for Purposes of ML or FT (applying c. 17.1-17.4 in R.17, c. IX.9)***

399. Persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to FT or ML can be held responsible under Article 165 StGB (because the ML provisions also contemplate the case of concealment and disguise of the proceeds, as well as possession) and Article 278d StGB respectively.

***Confiscation of Currency Related to ML/FT (applying c. 3.1-3.6 in R.3, c. IX.10)***

400. As previously mentioned, Article 17c of the ZollR-DG states that when “certain facts give rise to the assumption that cash or equivalent means of payment are introduced for the purpose of ML or FT, the Customs authorities are authorized in case of danger to seize the cash or means of payments.” In such cases the Customs authorities have to report immediately to the public prosecutor’s office, which can either dismiss or apply a sequestration in the conditions envisaged by Article 115 of the StPO (discussed earlier).

401. Confiscation of profits (Article 20 StGB) or forfeiture (Article 20b StGB) can be applied, if it can be proved that the money or bearer negotiable instruments are at the disposal of a criminal organization or a terrorist group, or they have been provided or collected as a mean for financing terrorism.

***Confiscation of Currency Pursuant to UNSCRs (applying c. III.1-III.10 in SR.III, c. IX.11)***

402. The seizure regime set forth by Article 17c of the ZollR-DG can be also applied in the case of FT. See also the discussion under paragraphs.

***Notification of Foreign Agency of Unusual Movement of Precious Metal and Stones (c. IX.12)***

403. The obligation to disclose upon request of the customs authorities applies also in the case of gold and other metals. The conditions for the exchange of information with third countries are laid out in the EC regulation No. 1889/2005 and in the various bilateral agreements signed by the Austrian Customs with their foreign counterparts. The authorities referred to a recent case involving a

shipment of platinum from Switzerland to Austria, in which they cooperated with the Swiss authorities (although the Austrian authorities believe that the case is related to VAT fraud rather than to ML).

***Safeguards for Proper Use of Information (c. IX.13)***

404. The information gathered through the declaration/disclosures procedures described above is subject to the Law on data protection (*Datenschutzgesetz, DSG*), which provides confidentiality requirements and the obligation to use the information gathered only for the purposes set forth by the law. This implies that data and information acquired from declarations is only used in the circumstances allowed for by Article 17c, paragraph 2 ZollR-DG.

***Additional Element—Implementation of SR.IX Best Practices (c. IX.15)***

405. See earlier Paragraphs in this section on the implementation of the SR.IX best practices and on the legal requirements. Authorities informed the assessors that the Police have canine units and that Customs are equipped with X-ray, scanners and endoscopes. At the beginning of 2009 the Austrian Customs authorities will start a project to train customs dogs to facilitate cash detection since the results of the use of canine units of other Austrian agencies in this regard are encouraging. Procedures are in place to detect cash couriers; according to the authorities. Risk- and intelligence-based controls reflecting passenger and destination profiles are used at Vienna airport, including information provided by the airports or gathered by direct access to the data bases of the airlines.

406. Procedures are in place for inspections, which are conducted by at least two persons. Technical equipment including photo documentation is standard of the Austrian Customs as well as secure handling, storage and accounting systems. To detect counterfeit currency the police has run seminars for customs officers. Guidelines for cooperation with judicial authorities are in place for a very long time, since the customs officers serve as judicial officers in case of penal investigations. In cases of ML or FT the competent police units (A-FIU and BVT) are consulted immediately in any case that has so far arisen.

***Additional Element—Computerization of Database and Accessible to Competent Authorities (c. IX.15)***

407. See discussion under Paragraph 351. The authorities informed that after the evaluation team declarations and detections electronically. The next step in progress is to get authorization for registration of this data bank in the Data Bank Register by the Data Protection Commission, which can be expected by December 2008. The request for registration specifically entails the provision of information to the A-FIU and the BVT. A pending issue is the development of the technical modalities for giving the A-FIU and the BVT access to the database.

**Effectiveness**

408. Although the legal framework is largely in line with SR.IX (with the exception of the municipalities Jungholz and Mittelberg, which are not in line with the requirements of SR.IX) the system is relatively recent, so no techniques/strategies (outside the more traditional controls aimed at detecting illegal smuggling of cigarettes or drug trafficking) have been yet developed to target and

tackle cash couriers. There is not yet a systematic use of the information gathered through the declaration/disclosure system to build up intelligence for AML/CFT purposes. The lack of a computerized database restrains the chances to target cash couriers. Only recently the Customs started to report to the A-FIU cases in which they suspect grounds of ML, but the number of reports is extremely low (in relation to the figures of declaration/disclosures which were provided, discussed later on).

409. From the statistics provided by the authorities on the figures of the declarations/disclosures it appears that the majority of the controls are done at the external EU-borders, so it can be questioned the effectiveness of the controls with the EU-borders. As previously mentioned, the authorities explained that at these borders the controls are not aimed at targeting cash couriers per se, but are only part of the controls routinely done in the actions against cigarette-smuggling or drug trafficking.

410. Also the volumes of declared cash are rather high, and it is interesting to note that in most cases the declarations are rendered on behalf of legal persons.

411. It also appears that the very few instances in which a seizure has been applied or a suspicious ML case was reported to the A-FIU were related to a failure to declare/disclose (rather than to cases in which the cash was declared and the authorities doubted about the legitimate origin of the cash). From the analysis of the statistics provided, the assessors have the impression that as long as the cash is declared the Customs authorities are content that a declaration was made and/or that sufficient explanations are provided for the purpose/on the origin (for example a case was described in which an individual goes regularly to a country that may pose a risk of ML, bringing each time cash amounting to EUR 800,000–1,000,000; the reason which was provided is that this person has a company in that country and prefers to avoid the banking system). This impression seems also confirmed by the fact that very few penalties have been applied since the introduction of these requirements.

412. As mentioned above, the borders with the municipalities of Jungholz and Mittelberg are completely free from any control under the requirements of SR.IX. The exemptions for these municipalities are of particular concern, not only because they are not in line with the requirements set forth by SR.IX, but because of the risk of ML, acknowledged by the authorities, associated to the transportation of cash from Germany into the 2 enclaves. Anecdotal evidence indicates that in Jungholz alone there are more than 15,000 bank accounts for a population of 300 inhabitants and that in the valley of Kleinwalsertal (where Mittelberg is located), there are several branches of banks for a population of 5,000 inhabitants, one of which claims to be the largest branch in Austria. The FMA indicated that the banking assets of one large credit institution are equivalent to EUR 1 billion.

### **2.7.2 Recommendations and Comments<sup>24</sup>**

413. The authorities should:

- Subject to disclosure or declaration obligations the transportation of cash or other bearer negotiable instruments into/out of the municipalities of Jungholz and Mittelberg;

---

<sup>24</sup> The FATF recognizes the EU as a supranational jurisdiction for the purposes of SR.IX, and that physical cross-border transportations of currency/BNI within the borders of the EU are to be considered domestic.

- Develop a computerized database for the storage of the information gathered through the declaration/disclosure process which should be used to build up intelligence to target cash couriers and to fight against ML/FT;
- Assess the risk and develop a strategy for containing the ML/FT risk associated to the transportation of cash or other bearer negotiable instruments into/out the municipalities of Jungholz and Mittelberg;
- Enhance cooperation between the customs and the A-FIU and develop a system to enhance the reporting of cases of cross-border transportation to the A-FIU.

### 2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors underlying rating
SR.IX	PC	<ul style="list-style-type: none"> <li>• Exception from the declaration/disclosure obligations for the municipalities of Jungholz and Mittelberg not in line with the requirements of SR.IX.<sup>25</sup></li> <li>• Lack of monitoring and checks of cross border transportation of cash into Jungholz and Mittelberg posing a serious risk of ML.<sup>26</sup></li> <li>• Implementation of the declaration/disclosure requirements not effective.</li> </ul>

### 3. PREVENTIVE MEASURE—FINANCIAL INSTITUTIONS

414. Customer due diligence (CDD) and record keeping requirements have been in place in Austria for several years. As an EU Member State, Austria was required to implement the Third EU ML Directive (Directive 2005/60/EC) and the implementing Directive (Directive 2006/70/EC) into its national legislation by 15 December 2007. New AML/CFT provisions were issued to this effect in 2007 and came into force on January 1 2008. They require financial institutions to adopt preventive measures adjusted to risks, and they provide for variable levels of CDD, depending on the risk of money laundering and terrorist financing, in more circumstances than was previously the case in Austria.<sup>27</sup> They also strengthened the previous identification requirements, added identification requirements with regard to the beneficial owners, and introduced new requirements to monitor transactions and relationships with politically exposed persons (PEPs) and cross-border correspondent banks.

<sup>25</sup> see footnote No 24.

<sup>26</sup> see footnote No 24.

<sup>27</sup> Austria adopted a limited risk-based approach for certain type of transactions or customer prior to the implementation of the third EU Directive: non-face-to-face business, for example, has been subject to enhanced due diligence since 2003 (former Article 40, paragraph 8 of the BWG).

### 3.1 Risk of Money Laundering or Terrorist Financing

415. As mentioned above, the transposition of the EU provisions into the domestic framework entailed the introduction of a risk-based approach. Financial institutions are required to conduct a risk-analysis of their business, using suitable criteria, and to take appropriate risk-based measures to ascertain customer information and conduct ongoing monitoring. In certain instances, applying the risk-based approach is framed by legal requirements, either particularizing criteria of risk, or allowing simplified CDD for low risk customers or transactions. CDD obligations are reduced for credit or financial institutions according to Article 1, paragraph 2 of the BWG, and under restricted conditions, fiduciary accounts held by attorneys at law or notaries, from EU Member States or third countries imposing equivalent AML/CFT measures and supervision. Enhanced due diligence is required from financial institutions on a risk-sensitive basis as a general practice, and is specifically required for situations the law considers as exhibiting higher level of ML/FT risks (non-face-to-face, cross-border correspondent banking, PEPs). The risk-based approach is modeled on the one set out in the EU Directive. It is not the result of a specific risk assessment of the Austrian financial sector. However, the characteristics of the Austrian legal framework, such as the possibility to issue shares in bearer form, and of the Austrian financial sector, such as a significant private banking industry, point to an elevated vulnerability to abuse for ML and FT purposes which is not mitigated by enhanced due diligence measures.

416. The assessment has been conducted on the basis of the legislation in force at the date of the onsite visit in September 2008 and immediately thereafter. It therefore covers the new AML/CFT legal framework which came into force on January 1 2008. Several of the FMA's operational circulars are still pending, and should be completed in the forthcoming months.

### 3.2 Customer Due Diligence, Including Enhanced or Reduced Measures (R.5 To 8)

#### 3.2.1 Description and Analysis

##### Legal Framework

417. All persons and entities who conduct as a business in Austria one or more of the financial activities listed in the FATF Glossary are subject to AML/CFT measures. The Austrian AML/CFT measures applicable to the financial sector are all set out in primary legislation, more precisely in the sector-specific laws: provisions for credit and domestic financial institutions are set out in the Banking Act (*Bankenwesengesetz*, BWG), provisions for the insurance companies in the Insurance Supervision Act (*Versicherungsaufsichtsgesetz*, VAG), and provisions for the securities firms in the Securities Supervision Act (*Wertpapieraufsichtsgesetz*, WAG). All three laws were recently amended to reflect the provisions of the Third EU ML Directive, with, as mentioned above, the new provisions coming into force in January 1 2008.

418. The supervisor for the financial sector, the Financial Market Authority (FMA), issued a number of Circulars (*Rundschreiben*), such as the Circular on Identification and Verification of Identity, which provide additional information on, as well as the FMA's interpretation of the AML/CFT measures set forth in the laws, mainly the BWG. The purpose of the Circulars is not to impose further measures but to clarify the legal requirements. While they are not binding and not

enforceable as such, non-compliance with the Circular could entail a level of non-compliance with the legal provisions and non-compliance which would be sanctioned on the basis of the law.

419. The BWG applies to all “credit institutions” and “financial institutions according to Article 1, paragraph 2 of the BWG”:

420. Credits institutions are institutions that are authorized by the FMA to carry out “banking transactions” under the Austrian laws. The definition of “banking transactions” is broad and covers not only the usual type of banking activities, but also further activities such as money exchange. More specifically, are considered banking transactions under the BWG any of the following activities carried out for commercial purposes:

1. The acceptance of funds from other parties for the purpose of administration or as deposits (deposit business);
2. The provision of non-cash payment transactions, clearing services and current-account services for other parties (current account business);
3. The conclusion of money-lending agreements and the extension of monetary loans (lending business);
4. The purchase of cheques and bills of exchange, and in particular the discounting of bills of exchange (discounting business);
5. The safekeeping and administration of securities for other parties (custody business);
6. The issuance and administration of payment instruments such as credit cards and traveler’s cheques;
7. Trading for one's own account or on behalf of others in:
  - a) Foreign means of payment (foreign exchange and foreign currency business);
  - b) Money-market instruments;
  - c) Financial futures contracts, including equivalent instruments settled in cash as well as call and put options on the instruments listed in lit. a and d to f, including equivalent instruments settled in cash (futures and options business);
  - d) Interest-rate futures contracts, forward rate agreements (FRAs), interest-rate and currency swaps as well as equity swaps;
  - e) Transferable securities (securities business);
  - f) Derivative instruments based on lit. b to e; unless these instruments are traded for private assets;
- 7a. Trading in financial instruments pursuant to Article 1, paragraph 1, no. 6, lit. e-g and j of the WAG for the credit institution's own account or on behalf of others, except in the case of trading conducted by persons pursuant to Article 2, paragraph 1, nos. 11 and 13 of the WAG;
8. The assumption of suretyships, guarantees and other forms of liability for other parties where the obligation assumed is monetary in nature (guarantee business);
9. The issuance of mortgage bonds, municipal bonds and covered bank bonds as well as the investment of proceeds from such instruments in accordance with the applicable legal provisions (securities underwriting business);
10. The issuance of other fixed-income securities for the purpose of investing the proceeds in other banking transactions (miscellaneous securities underwriting business);

11. Participation in underwriting third-party issues of one or more of the instruments listed under no. 7 lit. b to f as well as related services (third-party securities underwriting business);
12. The acceptance of building savings deposits and the extension of building loans in accordance with the Building Society Act (*Bausparkassengesetz, BSpG*) (building savings and loan business);
13. The management of investment funds in accordance with the Investment Fund Act 1993 (*Investmentfondsgesetz, InvFG*) (investment fund business);
- 13a. The management of real estate investment funds in accordance with the Real Estate Investment Fund Act (*Immobilien-Investmentfondsgesetz, ImmoInvFG*), (real estate investment fund business);
14. The establishment or management of participation funds in accordance with the Participation Fund Act (*Beteiligungsfondsgesetz*) (participation fund business);
15. The business of financing through the acquisition and resale of equity shares (capital financing business);
16. The purchase of trade receivables, assumption of the risk of non-payment associated with such receivables – with the exception of credit insurance – and the related collection of trade receivables (factoring business);
17. The conduct of money brokering transactions on the interbank market;
18. The brokering of transactions as specified in
  - a) No. 1, except for transactions conducted by contract insurance undertakings;
  - b) No. 3, except for the brokering of mortgage loans and personal loans by real estate agents, personal loan and mortgage loan brokers, and investment advisors;
  - c) No. 7 lit. a where this applies to foreign exchange transactions;
  - d) No. 8.
19. The issuance of electronic money (e-money business);
20. The acceptance and investment of severance payment contributions from salaried employees and self-employed persons (severance and retirement fund business);
21. The purchase of foreign means of payment (e.g., notes and coins, cheques, traveler's letters of credit and payment orders) over the counter and the sale of foreign notes and coins as well as traveler's cheques over the counter (exchange bureau business);
22. The transfer of funds, except for physical transports, by accepting money or other means of payment from the originator and paying out a corresponding amount in money or other means of payment to the beneficiary by way of non-cash transfer, communication, credit transfer or other uses of a payment or clearing system (remittance services business).

421. All “credit institutions” are supervised by the FMA (Article 69, paragraph 1 of the BWG. See write-up on Recommendation 23 for more details).

422. “Financial institution”, in the Austrian legislation, refers to an institution which is not a credit institution and which conducts one or more of the following activities for commercial purposes if they are conducted as the institution's main activities:

- leasing business;

- provision of advice to undertakings on capital structure, industrial strategy and related questions, as well as advice services related to mergers and the purchase of undertakings;
- provision of credit reporting services; and
- the provision of safe deposit services (Article 1, paragraph 2 of the BWG).

423. With the terms “[carried out] for commercial purposes”, the BWG uses the same wording as the Value Added Tax Act (UStG). The Austrian Administrative Court (*Verwaltungsgerichtshof, VwGH*) ruled that the notion of “[carried out] for commercial purposes” covers all activities “that are sustainably aimed at generating earnings”, including when the activity itself does not generate earnings: it is sufficient that the activity generates earnings indirectly. This was for example the case in VwGH 21.05.2001, 2000/17/0134 where the VwGH qualified written guarantees, which the bank issued as a “free service” for its customers, as banking activities carried out for commercial purposes, because the guarantees served the purpose of intensifying existing customer relationships and were thereby aimed at generating future earnings. According to the Court, there must however be an element of “sustainability” in the activity carried out. This may already be the case when (i) there is one relevant activity and (ii) it can be concluded from objective circumstances that there is the intention to repeat the activity (see e.g., VwGH 25.1.1995, 93/13/0084 ÖJZ 1996/106 F). In light of this jurisprudence, the courts have considered in some instances that an activity conducted on a single occasion was “carried out for commercial purposes” when they deemed that the intention was to establish a long-term customer relationship.

424. “Financial institutions” referred to in Article 1, paragraph 2 of the BWG are supervised not by the FMA, but by local district authorities.

### **Terminology**

425. As mentioned above, the Austrian definition of “credit institutions” is broad and covers persons or institutions that deal with most of the financial activities listed under the FATF definition of financial institutions, while the definition of “financial institutions” is narrow and refers only to persons or entities that are not “credit institutions” and that conduct one or more of a limited list of activities mentioned in Article 1, paragraph 2 of the BWG. To avoid confusion and to ensure consistency with the terminology adopted in the standard, the present report uses the terms:

- “credit institution”, or, where relevant, “banks” when referring to those institutions that carry out the activities listed in Article 1, paragraph 1 of the BWG;
- “domestic financial institutions” when referring to those institutions covered by Article 1, Paragraph 2 of the BWG; and
- “financial institutions” when referring to financial institutions in the FATF sense, that is, when referring to credit institutions, domestic financial institutions, insurance undertakings (but not insurance intermediaries) and securities firms.

426. For the purposes of this report, all AML/CFT provisions applicable to credit and/or domestic financial institutions, set forth in Articles 40, 40a- 40d and 41 of the BWG, are described under the subtitle “Credit and domestic financial institutions.”

427. The VAG applies to domestic insurance undertakings (i.e., undertakings whose head offices are situated in Austria) and foreign insurance undertakings (i.e., undertakings with head offices outside Austria) when the insurance contracts are concluded within Austria or advertised in Austria (Article 1 of the VAG). Measures intended to prevent ML/FT are set out under Article 98a-98h of the VAG. They are applicable to “insurance undertakings within the scope of the operation of the life assurance business” (Article 98a, paragraph 1 VAG) and are described in this report under the subtitle “Insurance undertakings.”

428. Insurance intermediaries are mostly self-employed persons who operate as insurance agents or brokers. For historical reasons, the insurance intermediaries are not subject to the VAG but to the Trade Act (*Gewerbeordnung, GewO*). One of the reasons that guided this choice was that, in view of the large number of intermediaries (18,374), the larger and decentralized organization of the trade authorities was deemed more appropriate for the conduct of supervision. The measures applicable to intermediaries are described under Recommendation 9.

429. The WAG applies to investment firms and investment services and activities companies. It does not explicitly address AML/CFT measures but makes instead, in its Articles 6 and 12, paragraph 4, a general reference to specific articles of the BWG, including its Articles 40, 40a, 40b, 40d and 41, and thus requires investment firms and investment services companies to implement the AML/CFT provisions of the BWG in the same way as credit and domestic financial institutions. All the identification requirements set out in the BWG therefore apply *mutatis mutandis* to the securities sector. It must be mentioned from the outset that while this cross-referencing generally applies without difficulty, there are some instances (highlighted in the relevant sections of this report) where it is neither entirely relevant nor adequate. The authorities indicated that their intention is to adjust the cross-referencing to the BWG made under Articles 6 and 12, paragraph 4 of the WAG by deleting the references to the provisions of the BWG that do not apply to securities firms. AML/CFT measures applicable to the sector are described in this report under the subtitle “Securities institutions.” The provisions of the BörseG which require the exchange operating company to report suspicious transactions are addressed under the relevant criteria in other sections of the report.

### ***Prohibition of Anonymous Accounts (c. 5.1)***

#### **Credit and Domestic Financial Institutions**

430. Anonymous accounts are prohibited in Austria both explicitly (Article 40d paragraph 2 of the BWG) and through the implementation of the identification requirements (Article 40, paragraph 1 BWG). More specifically, the BWG prohibits credit institutions and domestic financial institutions from maintaining anonymous accounts and from accepting anonymous savings deposits (“inadmissible business relationships”, Article 40d paragraph 2 of the BWG). It also sets out a series of identification requirements (described under criterion 5.2 below) that further prevent anonymous accounts as well as the opening of accounts under fictitious names. Article 40d of the BWG came into force on January 1, 2008 (Article 107, paragraph 55 of the BWG). Various levels of identification have, however, been required for much longer:

- Mandatory identification requirements regarding non-residents were passed in 1991;

- Mandatory identification requirements for all customers and specific identification provisions for *Treuhand* (identification of *Treugeber* and *Treuhänder*) were adopted in 1993;
- Mandatory identification requirements for securities accounts were adopted in 1996; and
- Mandatory identification requirements for savings accounts were adopted in 2000.

431. Addressing concerns raised by the FATF with respect to transparency of anonymous passbooks, the authorities enacted amendments to the BWG in 2000 which prohibit the opening of new anonymous savings deposit accounts, and subject existing anonymous savings deposit accounts to special diligence transactions. Savings deposits are funds deposited with credit institutions for the sole purpose of investment and, “as such can only be accepted against the delivery of certain documents (savings documents)” (Article 31, paragraph 1 of the BWG). They carry different denominations depending on the financial entity that issues them (*Sparbuch*, *Sparbrief*, *Sparkassenbuch* etc.). All withdrawals from savings deposits can only be made in cash at the counter, as funds can be transferred to -but not from- a savings deposit (Article 32, paragraph 3 of the BWG).

432. Credit and domestic financial institutions must ascertain and verify the customer’s identity:

- before initiating savings deposit transactions; these transactions must always be considered as permanent business relationship and subject to full CDD requirements (Article 40, paragraph 1, no. 1 of the BWG);
- before receiving any deposit or operating any withdrawal amounts to at least EUR 15,000 or an equivalent value (Article 40, paragraph 1, no. 4, and paragraph 6 of the BWG); and
- when there are reasonable grounds to suspect terrorist financing or money laundering, or when there are doubts as to the veracity or adequacy of previously obtained identification data (Article 40, paragraph 1, nos. 3 and 5 BWG).

433. Although savings documents cannot be established under a name other than that of the customer identified, pursuant to Article 40, paragraph 1, they can be issued with “a certain designation” (Article 31, paragraph 1 of the BWG). According to the authorities, this could include for example a designation such as “wedding” in the case of a savings deposit account offered on the occasion of a wedding. The authorities also confirmed that the initial customer must nevertheless be identified in all cases.

434. Banks may open and maintain numbered accounts at the request of customers. Although the CDD rules apply to these and other customers in the same way, the identification data is only available to a limited number of persons within the bank, typically the relationship manager, the compliance officer and senior managers. Clients may also request that all banking correspondence be kept at the bank instead of being mailed to them. Some of the banks met by the assessors indicated that they held numbered accounts but none considered them as a factor of risk. Indeed, none of the included numbered accounts or the holding of banking correspondence are considered as risk criteria for the opening and monitoring of business relationships.

## **Insurance Undertakings**

435. While the VAG does not specifically prohibit anonymous contracts or contracts under fictitious names, the identification requirements set out in its Article 98b adequately preclude anonymous contracts and contracts under fictitious names.

## **Securities Institutions**

436. Pursuant to Articles 6 and 2, paragraph 4 of the WAG, the provisions of Articles 40, 40a, 40b, 40d and 41 are applicable to investment firms and investment services companies. The prohibition described above therefore applies, as well as the identification requirements described below.

### ***When is CDD required (c. 5.2)***

#### **Credit and Domestic Financial Institutions**

437. Pursuant to Article 40, paragraph 1 BWG, credit and domestic financial institutions are required to ascertain and verify the identity of the customer:

- before initiating a permanent business relationship;
- before carrying out an occasional transaction of EUR 15,000 (or an equivalent value) or more (regardless of whether the transaction is carried out in a single operation or in multiple operations between which there is an obvious connection);
- if the institution suspects or has reasonable grounds to suspect that the customer belongs to a terrorist organization or the customer objectively participates in transactions which serve the purpose of money laundering or terrorist financing;
- for every deposit into and every withdrawal from savings deposits if the amount deposited or withdrawn comes to at least EUR 15,000 or an equivalent value;
- when there are doubts as to the veracity or adequacy of previously obtained customer identification data.

438. Pursuant to the EU Regulation No. 1781/2006, credit and domestic financial institutions in Austria must also identify the customer and ensure that complete originator information is included in cross-border wire transfers (see write-up under Special Recommendation VII for more details).

439. In its Circular on Identification and Verification of Identity, the FMA provides further definitions and explanation to expound on the provisions of the law: It defines “ascertaining identity” as meaning “obtaining information on the identity of the natural or legal person to be identified” and “verifying the identity” as “validating the information on identity obtained against meaningful supporting documents and information.” It also provides that “ascertaining and verifying the identity may be performed at the same time, and thus it is not always possible to clearly separate these two procedures. Information on identity must be documented. The obligation to keep information stipulated in Article 40, paragraph 3, no. 1 BWG applies in this case.”

## **Insurance Undertakings**

440. Article 98b, paragraph 1 of the VAG provides similar requirements as those set out in Article 40, BWG, with the exception of the provisions dealing with savings account which have not been duplicated in the VAG since they are not relevant to the insurance business.

## **Securities Institutions**

441. Article 12, paragraph 4 of the WAG requires investment companies and investment services companies to implement the provisions of Article 40, of the BWG. The securities sector is therefore subject to the provisions described above (although the provision of Article 40, paragraph 1, no. 4 of the BWG dealing with savings deposits does not apply to the securities sector).

### ***Identification measures and verification sources (c. 5.3)***

#### **Credit and Domestic Financial Institutions**

442. Credit and domestic financial institutions are required by the BWG to ascertain the identity of the customer on the basis of the personal presentation of an official photo identification document by the customer (Article 40, paragraph 1 of the BWG). Are considered to be “official photo identification documents”, documents which are issued by a government authority and which bear a non-replaceable and recognizable photograph of the head of the person in question, and which include the name, date of birth and signature of the person as well as of the authority that issued the document. In the case of foreign passport, the passport need not contain the person’s complete date of birth if this complies with the law of the country that issued the passport. If the customer is not legally competent, the identity of his or her legal representative must be sought and verified.

443. The authorities noted that official documents that do not enable a clear facial recognition of the customer (such as for example passports including photographs of veiled persons) are not deemed sufficient for identification purposes. It also expounded on these requirements in its Circular on Identification and Verification of Identity, paragraphs 24-36. Unless identification may be ascertained on the basis of other documents issued by government authorities, the credit and domestic financial institutions may not establish a business relationship or execute an occasional transaction above the legal threshold.

444. The law (Article 40, paragraph 1 *in fine* of the BWG) provides two exceptions to the general identification and verification requirements:

- in case of reliance on other credit or financial institutions to carry out the identification procedures (although the ultimate responsibility for compliance with the identification requirements remains with the initial credit or financial institution); and
- in cases where the customer itself is a credit or financial institution supervised for compliance with similar identification obligations, as described under Article 40a, paragraph 1 of the BWG.

445. Both instances are described in more detail under the simplified CDD measures below.

446. While there is no requirement in the law to maintain a copy of the identification document provided by the customer, the authorities maintain that it is common practice for credit and domestic financial institutions to include a copy of the documents in their files as a means to prove to the supervisor that they have adequately fulfilled their identification requirements.

### **Insurance Undertakings**

447. The identification and verification requirements in the insurance sector are set out in Article 98b, paragraph 1 of the VAG in the same terms as in Article 40, paragraph 1 of the BWG. The measures described above therefore also apply to the insurance undertakings, including the exemptions (see write-up on simplified due diligence).

### **Securities Institutions**

448. The provisions of Article 40, paragraph 1 of the BWG described above apply *mutatis mutandis* to the investment companies and investment service companies (Articles 6 and 12, paragraph 4 of the WAG).

### ***Identification of Legal Persons or Other Arrangements (c. 5.4)***

### **Credit and Domestic Financial Institutions**

449. When dealing with legal persons, credit and domestic financial institutions are required by law to identify the natural person authorized to represent the legal entity (on the basis of a official photo identification document) and his or her powers to represent the legal entity (Article 40, paragraph 1 of the BWG). They must also identify the legal person itself on the basis of “meaningful supporting documentation which is available under the usual legal standards of the country in which the legal person is incorporated.” For legal persons incorporated in Austria, this would entail seeking an extract of the Commercial Register.

### **Insurance Undertakings**

450. The wording of Article 98b of the VAG with respect to the identification of legal persons is similar to that of the BWG described above.

### **Securities Institutions**

451. The measures described under the credit and domestic financial institutions are directly applicable to the investment firms and investment services companies (Articles 6 and 12, paragraph 4 of the WAG).

### **Effectiveness**

452. During discussions with financial institutions from all three sectors, the assessors were told that CDD measures are applied before entering into a permanent business relationship or conducting a one-time transaction above EUR 15,000. Most institutions use a questionnaire to collect information which is filled out either by the relationship manager or by the customer. Data generally include information related to the identity, as well as the activity of the client, and excerpts from the

Commercial Register. Verifications are conducted on risk basis to ensure a satisfactory level of confidence in the accuracy of information provided. Investigations aim at ensuring consistency of all data provided and collected, and involve mostly checking external databases, as well as internet, notably for nonresident customers.

453. Financial institutions consider that their exposure to ML/FT risks is very low in their domestic or EU activities, but higher with respect to their activities within the CESE and the CIS. For Austria, they take comfort from their proximity to their clients and the overall limited typologies of ML/FT, based on few cases and fewer convictions. Some institutions, mostly internationally active banks, have initiated formal assessments of their risk profile, categorized some type of business as higher risks, and defined specific verification procedures adjusted to the risk. In other financial institutions, the risk analysis of the business, required under the new legal provisions, is being implemented. All institutions draw comfort from their screening process at the inception of relationships, and choose to decline new business where information provided or collected is not fully satisfactory. While required by the BWG to consider sending a report to A-FIU in such cases (Article 40, paragraph 2d), they do not routinely file an STR on these attempted operations. Many of them mentioned contacting the A-FIU by phone. Indeed, the A-FIU informed the assessors that it received at least 50 STRs in 2008 which were filed in relation to either terminating, or declining taking up a business relationship. It is worth noting that most financial institutions seem to refer to country risk as the country of residence, or of origin, and less often to the country where the income or the wealth is generated.

### ***Identification of Beneficial Owners (c. 5.5; 5.5.1 & 5.5.2)***

#### **Credit and Domestic Financial Institutions**

454. Financial institutions are required by law to ask the customer whether he or she is acting on behalf on another person (Article 40, paragraph 2 BWG). The law also obliges the customer to comply with the request and provide the credit or financial institution with evidence of the identity of the “trustor” by the presentation of the original or a copy of the “trustor’s” official photo identification document. The FMA defined the term “trustor” in paragraph 77 of its Circular on Identification and Verification of Identity as “the natural or legal persons for whose account or on whose behalf a business relationship is established or a transaction is executed.” It also provides that “like the beneficial owner of a legal person, the trustor is the beneficiary of the banking transaction conducted on his behalf” (paragraph 79). The customer acting on behalf of another person must also submit a written declaration stating that he or she has ascertained the identity of the “trustor” personally or through reliable sources. Are considered “reliable sources”, courts and other government authorities, notaries, attorneys at law, and other credit or financial institutions. The customer himself or herself must be identified in person. Identification of the trustee by a third party is explicitly ruled out by Article 40, paragraph 2 of the BWG. The identity must be verified in such a way that the obliged entity is satisfied that it knows who the beneficial owner is, and has an understanding of the ownership and control structure of the customer (Article 40, paragraph 2a of the BWG). The authorities confirmed that the ultimate responsibility for the identification of the “trustor” remains with the credit or financial institution and that the latter may not initiate or pursue business activities with the customer in cases where the customer did not establish adequately the identity of the person he or she is acting on behalf of.

455. In the case of special fiduciary accounts of authorized real estate administrators acting on behalf of joint ownership associations for real estate properties, the presentation of an extract of the property register is considered valid evidence of the trustor's identity in the case of joint owners who are natural persons (Article 40, paragraph 2 *in fine* BWG).

456. Article 40, paragraph 2(a), no. 1 of the BWG goes further by requiring credit and domestic financial institutions to call upon the customer to reveal the identity of the customer's beneficial owner and to take risk-based and appropriate measures to verify the identity of the beneficial owner. The BWG defines beneficial owner in comprehensive terms, as follows:

"the natural persons who ultimately own or control the customer. In particular, the term" "beneficial owner" includes the following:

- a) in the case of corporate entities:
  - aa) the natural persons who ultimately own or control a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including ownership or control through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 percent plus one share is considered sufficient to meet this criterion;
  - bb) the natural persons who otherwise exercise control over the management of a legal entity;
- b) in the case of legal entities such as foundations, and in the case of trusts which administer and distribute funds:
  - aa) where the future beneficiaries have already been determined, the natural persons who are the beneficiaries of 25 percent or more of the property of a trust or legal entity;
  - bb) where the individuals who benefit from the trust or legal entity have yet to be determined, the class of persons in whose main interest the trust or legal entity is set up or operates; and
  - cc) the natural persons who exercise control over 25 percent or more of the property of a trust or legal entity."

457. While the obligation set out in Article 40, paragraph 2 BWG (identification of the "trustor") has been in place since 1993, the provisions requiring the identification of the beneficial owner are more recent and came into force on January 1, 2008 as part of the implementation package of the Third EU ML Directive.

458. Despite the above, pursuant to Article 31, paragraph 3 of the BWG, savings deposits which amount to less than EUR 15,000 may be registered under a different designation than the customer's name. In such a case, the party who presents the savings documents to access to the savings deposits must provide the password defined by the customer. There is no requirement for credit institutions to obtain and take reasonable measures to verify the identity of the holder of the savings documents, that is, the beneficial owner. Credit institutions that the assessors met have not implemented identification

and verification procedures for those persons. There is no limitation to the number of savings deposit accounts that a customer may open under a certain designation.

### **Insurance Undertakings**

459. Like credit and domestic financial institutions, insurance undertakings are explicitly required by the law to ask the person who intends to establish a customer relationship whether he or she is acting as a “trustee”, that is, on behalf of another person, the “trustor.” If the customer declares acting as a trustee, he or she must be identified in person by the insurance company. Identification of the trustee by a third party is explicitly ruled out. The trustee must also “furnish proof of the trustor’s identity to the insurance undertaking.” Under the provisions of the law, this may be done by presenting the original or a copy of the trustor’s official photo identification document, in the case of natural persons, or, in the case of legal persons, “by means of meaningful supporting documents which are available pursuant to the legal standard prevailing in the country of the head office of the legal person” (Article 98b, paragraphs 2 and 1 of the VAG).

460. Pursuant to Article 98b, paragraph 3 of the VAG, insurance undertakings must ask the customer to make known the identity of the beneficial owner, and take risk-based and adequate measures to verify his or her identity so that they are satisfied that they know who the beneficial owner is, “including, as regards legal persons and trusts, take risk-based and adequate measures to understand the ownership and control structure of the customer.” “Beneficial owner” is defined in line with the standard as follows (Article 98a, paragraph 2, no. 3 of the VAG). “Beneficial owner” shall mean the natural persons who ultimately own or control the customer. The term of “beneficial owner” shall include in particular:

- a) in the case of corporate entities:
  - aa) the natural persons who ultimately own or control a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 percent plus one share shall be deemed sufficient to meet this criterion;
  - bb) the natural persons who otherwise exercise control over the management of a legal entity;
- b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
  - aa) where the future beneficiaries have already been determined, the natural persons who are the beneficiaries of 25 percent or more of the allocations of a trust or legal entity;
  - bb) where the individuals that benefit from the trust or legal entity have yet to be determined, the class of persons in whose main interest the trust or legal entity is set up or operates;
  - cc) the natural persons who exercise control over 25 percent or more of the property of a trust or legal entity.

### **Securities institutions**

461. The provisions dealing with the beneficial owner described under the credit and domestic financial institutions section above are also applicable to the securities institutions (Articles 6 and 12, paragraph 4 of the WAG).

### **Effectiveness**

462. The requirements to identify the beneficial owner, as defined in the writing for criterion 5.5 and especially in 5.5.2, are recent and came into force on January 1, 2008. Financial institutions are in the process of applying these new requirements to their existing portfolio. The most commonly used approach is to collect beneficial owner information from the customer and to conduct simple investigations (such as searches in databases or on the internet) to ensure the plausibility of data. All financial institutions interviewed also mentioned that they hold very few accounts for legal arrangements such as foundations, and that, in such circumstances, they would be able to ascertain the natural persons who are the beneficial owners, as required under the new legislation.

### ***Information on Purpose and Nature of Business Relationship (c. 5.6)***

#### **All Financial Institutions**

463. Credit and domestic financial institutions, insurance undertakings and securities institutions are all required to take risk-based and appropriate measures to obtain information on the purpose and nature of the intended business relationship (Article 40, paragraph 2a, no. 2 of the BWG; Article 98b, paragraph 3, no. 2; Articles 6 and 12, paragraph 4 of the WAG).

464. This requirement came into effect on January 1 1 2008. At the time of the assessment, financial institutions appeared to have integrated the required information into their overall assessment of the customer, without however having formally defined risk levels and related diligences.

### ***Ongoing Due Diligence on Business Relationship (c. 5.7; 5.7.1 & 5.7.2)***

#### **All Financial Institutions**

465. The BWG, VAG and WAG (by reference to the BWG) explicitly require credit and domestic financial institutions, insurance undertakings, investment firms and investment services companies “to take risk-based and adequate measures to conduct ongoing monitoring of the business relationship.” They also specify that ongoing monitoring includes scrutiny of transactions undertaken throughout the course of the relationship, and aims at ensuring that the transactions conducted are consistent with the institutions’ knowledge of the customer, the customer’s business and risk-profile, including, where necessary, the source of funds, and to ensure that the documents, data or information held are kept up to date (Article 40, paragraph 2a, no. 3 of the BWG; Article 98b, paragraph 3, no. 3 of the VAG; Articles 6 and 12, paragraph 4 of the WAG).

## **Effectiveness**

466. These legal provisions also came into effect on January 1, 2008. They built upon previous provisions by introducing a broader obligation to monitor business relationships and by requiring to do so on a risk-adjusted basis. To satisfy these requirements, financial institutions must implement enhanced monitoring systems, using generally software available on the market. Several institutions pooled together to develop common tools through a joint IT company. Development and testing of risk matrix were underway at the time of the evaluation. More advanced multinational financial institutions also felt the need to upgrade their existing systems in line with the new obligations.

### ***Risk—Enhanced Due Diligence for Higher Risk Customers (c. 5.8)***

467. All three laws (BWG, VAG and WAG by reference to the BWG) call for enhanced due diligence in two types of circumstances: (i) situations in general “which by their nature can present a higher risk of money laundering or terrorist financing” (Article 40b, paragraph 1 of the BWG; Article 98d, paragraph 1 of the VAG, and Articles 6 and 12, paragraph 4 of the WAG); and (ii) circumstances explicitly enumerated in the laws (Article 40b, paragraph 1, nos. 1 to 3 of the BWG; Article 98d, of the VAG; Articles 6 and 12, paragraph 4 of the WAG). The specific measures that are required to be complied with in addition to the standard CDD obligations are however only listed in the second type of circumstances. It is up to the financial institutions to decide what type of additional measures are adequate in other situations that they identified as posing a higher risk. The specific circumstances where additional customer due diligence measures must be undertaken are described below:

### **Credit and Domestic Financial Institutions**

468. Article 40b, paragraph 1, nos. 1 to 3 of the BWG classifies three types of situations as higher risk and, in each case, requires that specific additional measures be taken to compensate the increased risk:

- non-face-to-face relationships, that is, when the customer is not physically present for identification purposes (see write up on Recommendation 8 for more details on the type of action required);
- cross-border correspondent banking, that is, business relationship with banks established in non-EU members (see write up on Recommendation 8 for more details on the type of action required); and
- transactions or relationships with politically exposed persons (PEPs) from any country other than Austria (see write up on Recommendation 6 for more details on the type of action required).

469. As mentioned above, there is also a general requirement to apply additional measures to situations which present a higher risk of money laundering of terrorist financing (Article 40b, paragraph 1 of the BWG). In this case however, the type of additional measures that the credit and domestic financial institutions should take has not been defined in the law or in guidance. It is therefore up to the institutions to decide what type of additional measures they deem reasonable and sufficient to mitigate the higher risk.

470. Other circumstances which are listed as examples of higher risk transactions or relationships by the Basel Committee in its CDD paper, in particular non-resident customers, private banking, customers that are personal assets holding vehicles (such as trusts for example), or customers that are companies that have nominee shareholders or shares in bearer form are not explicitly categorized as higher risk transactions or relationships in Austria. It therefore falls upon the institutions to decide in each case whether the risk is higher than the average. However, none of the credit and domestic financial institutions interviewed during the mission noted applying additional CDD measures to these cases.

### **Insurance Undertakings**

471. In addition to the general requirement to take measures in situations that present a higher risk, the VAG lays out two types of circumstances where insurance undertakings must take additional CDD measures: non-face-to-face businesses and transactions or business relationships with PEPs. In both cases, the measures required are the same as those listed in the BWG (described in detail in the write up on Recommendations 8 and 6).

### **Securities Institutions**

472. Articles 6 and 12, paragraph 4 of the WAG refer to the BWG—in other words, the provisions described above apply *mutatis mutandis* to the securities sector.

473. As mentioned above, both the BWG and the VAG establish a general obligation to apply enhanced due diligence measures to situations of higher ML/FT risk. However, integral to the development of customer monitoring is the definition of specific risk criteria resulting in enhanced diligence. At this early stage of implementation, many financial institutions refer to the limited number of higher risk criteria described in the law, essentially PEPs, non-face-to-face, conditions of payment (single premium) etc. No consideration has been given by the Austrian legislator to additional higher risk criteria such as those given as examples in the FATF methodology, although they could be relevant to the type of business conducted by Austrian financial institutions.

### ***Risk—Application of Simplified/Reduced CDD Measures when appropriate (c. 5.9)***

#### **Credit and Domestic Financial Institutions**

474. Article 40a, of the BWG appears under the heading “Simplified customer due diligence obligations.” It provides that “by way of derogation from Article 40, paragraph 1, nos. 1, 2, and 5, and paragraphs 2 and 2a [i.e., the standard CDD measures], the obligations indicated in those provisions do not apply” in a certain number of circumstances listed in the same Article. More specifically, the standard CDD obligations do not apply in cases where:

- the customer is a credit institution or financial institution pursuant to Article 1, paragraphs 1 and 2 or pursuant to Article 3 of Directive 2005/60/EC, or a credit institution or financial institution situated in a non EU country which imposes obligations equivalent to those set forth in Directive 2005/60/EC and supervised for compliance with such obligations;
- provided that the risk of money laundering and terrorist financing is considered low in accordance with paragraph 4 if the customer(s) is (are):

1. exchange-listed companies whose securities are admitted to listing on a regulated market in one or more Member States, or exchange-listed companies from third countries which are subject to disclosure obligations pursuant to a regulation to be issued by the FMA on the basis of its power to issue regulations pursuant to Article 85, paragraph 10 Stock Exchange Act and such disclosure obligations are equivalent or comparable to those set forth in Community legislation;
2. domestic authorities; or
3. authorities or public bodies:
  - a) if they are entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation;
  - b) the identity of which is publicly available, transparent and certain;
  - c) the activities and accounting practices of which are transparent; and
  - d) if they are accountable either to a Community institution or to the authorities of a Member State, or appropriate check and balance procedures exist ensuring control of the customer's activity. (3) paragraph 2 also applies to:
    1. customers with regard to electronic money (Article 2, no. 58) where, if the device cannot be recharged, the amount stored in the device is no more than EUR 150, or where, if the data medium can be recharged—a limit of EUR 2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1,000 or more is redeemed in the same calendar year by the bearer pursuant to Article 6 E-Money Act or pursuant to Article 3 of Directive 2000/46/EC;
    2. savings activities for classes of school pupils, subject to the condition that the cooperation of the legal representative is not required in the identification of the school pupil and that, unless Article 40, paragraphs 1, 2 or 2a is applied in its entirety,
      - a) in the case of savings deposit accounts which are opened for individual minors, identification can be performed by the school pupil himself/herself in the presence of a teacher or through a teacher as a trustee; the identification data of the school pupils can be ascertained by the credit institution on the basis of their school identification cards, copies of their school identification cards or a list containing the names, dates of birth and addresses of the pupils in question;
      - b) in the case of collective savings deposits for school classes, the identification of the minor school pupils entitled to the savings deposit can be performed by a teacher as a trustee using a list containing the names, dates of birth and addresses of the pupils in question.

475. Despite the clear wording of Article 40a, of the BWG, the authorities stated that the intention of the legislator was not to create an exemption but to introduce an option for the application of simplified due diligence. No guidance has been issued to clarify this discrepancy, but the authorities intend to address it further.

476. Article 40a, Paragraph 4 further mentions that in assessing whether the customers or products and transactions indicated in paragraphs 2 and 3 represent a low risk of money laundering or terrorist financing, credit institutions and financial institutions must pay special attention to the activities of such customers and to the types of products and transactions which may be regarded as particularly likely, by nature, to be used or misused for ML/FT purposes. If available information suggests a ML/FT risk, the credit institutions and financial institutions are prohibited from classifying the customers or products and transactions in a low-risk category and must, consequently, apply the standard CDD measures.

477. A further exception is provided in Article 40a, paragraph 5 of the BWG in the case of fiduciary accounts held by attorneys at law or notaries, from Austria or any other country, that are subject to AML/CFT requirements and supervision equivalent to those of the international standards. In these cases, evidence of the identity of each individual “trustor” need not be provided to the credit institution or financial institution if the following requirements are fulfilled:

1. individual verification is infeasible due to the representation of large co-ownership communities of changing composition;
2. the ‘trustee’ submits a written declaration to the credit institution stating that he/she has identified his/her clients in accordance with Article 40, paragraphs 1, 2 and 2a, nos. 1 and 2 or the requirements of Directive 2005/60/EC, that he/she has stored the corresponding documents and will present them to the credit institution upon request;
3. the ‘trustee’ provides the credit institution with complete lists of the clients assigned to each fiduciary account within two months after the end of each calendar year;
4. the ‘trustor’ does not have his/her place of incorporation or place of residence in a noncooperative country or territory; and
5. no suspicion pursuant to Article 40, paragraph 1, no. 3 exists.

478. The second and third conditions listed above (provision by the trustee of a written declaration attesting that he or she has identified the clients and of a complete list of clients) do not apply “to clients for whom the respective individual transaction conducted or whose share of the claim on the respective trustee arising from fiduciary accounts does not amount to a total of EUR 15,000.” In other words, the law explicitly exempts these circumstances from any CDD as long as there is no suspicion of money laundering or terrorist financing and the trustor is not domiciled in a “noncooperative country.”

479. The authorities also pointed out that all “trustees” are clients of specific lawyers or notaries and thus have been identified pursuant to the lawyers’ and notaries’ CDD requirements.

480. Credit and domestic financial institutions are required to assess the level of risk of money laundering and terrorism financing before they may consider themselves exempted from applying the

full CDD measures. However, no mention to the risk of ML and FT is made in the case of the first exception, that is, with respect to credit and domestic financial institutions subject to equivalent AML/CFT measures. In other words, credit and domestic financial institutions (as well as securities firms) are fully exempt of any identification requirements when dealing with a foreign credit or financial institutions regardless of the level of risk. They are also exempt from any CDD measures when dealing with fiduciary accounts under EUR 15,000 when there is no risk of ML/FT. Rather than providing for “simplified” due diligence measures, as the heading of Article 40a, suggests, the law creates blanket exemptions from the identification requirements under its paragraph 1. This approach is not in line with the FATF standard whereby minimum CDD should nevertheless be accomplished, including in circumstances where the risk of money laundering and terrorist financing is low (thus requiring a certain level of prior risk assessment in all cases). The exemptions are of concern because they create loopholes in the Austrian system that criminals may misuse.

### **Insurance Undertakings**

481. Article 98c of the VAG contains, under the title “simplified customer due diligence”, provisions that are very similar to those set forth in the BWG. In addition to the general similarity with the BWG, the wording of the VAG addresses some aspects that are specific to the insurance sector: insurance undertakings have been added to the list of institutions that do not require identification (Article 98c, paragraph 1, nos. 1a and 1b) and a minimum threshold has been set. In addition to the circumstances described above, insurance undertakings are exempted from identifying the customer with respect to the following insurance contracts and related transactions:

- life insurance contracts where the annual premium is no more than EUR 1,000 or the single premium is no more than EUR 2,500;
- insurance contracts for pension schemes if there is no surrender clause and they cannot be used as collateral for a loan (Article 98c, paragraph 1, no. 2 of the VAG).

482. Like the BWG, the content of Article 98c of the VAG entails an exemption from CDD requirements rather than a simplification of standard CDD. For the reasons explained above, this is not in line with the standard.

### **Securities Institutions**

483. The provisions applicable to the credit and domestic financial institutions apply *mutatis mutandis* to securities institutions (Articles 6 and 12, paragraph 4 of the WAG). The write-up pertaining to the credit and domestic financial institutions (above) therefore applies to the securities sector as well. In this case, the wording of the BWG is not entirely relevant to the securities sector and it is unclear whether the securities firms consider that the exemption for “credit institutions” set out in the BWG addresses securities institutions per analogy. The authorities confirmed however that, despite Articles 6 and 12, of the WAG, the exemptions set out in the BWG do not apply to the securities sector.

### ***Risk—Simplification / Reduction of CDD Measures relating to overseas residents (c. 5.10)***

### **All Financial Institutions**

484. The BWG and VAG lists of circumstances where simplification of (and exemption from) the standard CDD requirements is possible are exhaustive. Simplified CDD is therefore not an option in situations other than those explicitly mentioned in the lists. The mere fact that customers reside abroad does not justify simplified CDD. The standard CDD obligations therefore apply.

***Risk—Simplified/Reduced CDD Measures Not to Apply when Suspicions of ML/FT or other high risk scenarios exist (c. 5.11)***

### **All Financial Institutions**

485. Pursuant to Article 40a, paragraphs 2 and 6 of the BWG, 98c, paragraph 1 of the VAG, Articles 6 and 12, paragraph 4 of the WAG, simplified CDD is not available in circumstances that present a suspicion of money laundering or of terrorist financing, except in the case laid out under Article 40a, paragraph 1 of the BWG (foreign credit and financial institutions subject to “equivalent” AML/CFT measures), where the exemption of CDD measures applies without the need for a prior risk assessment.

***Risk Based Application of CDD to be Consistent with Guidelines (c. 5.12)***

### **All Financial Institutions**

486. At the time of the assessment, no guidelines had been issued on the risk-based approach adopted in the laws. The FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorism Financing (June 2007) was circulated by the MoF to the Austrian financial institutions, via the WKO. The FMA is preparing a circular that will provide financial institutions with guidance on applying CDD measures on a risk-sensitive basis.

***Timing of Verification of Identity—General Rule (c. 5.13); Timing of Verification of Identity—Treatment of Exceptional Circumstances (c.5.14 & 5.14.1)***

487. As mentioned above (see write-up on criterion 5.2), credit and domestic financial institutions, as well as insurance undertakings and securities firms, must identify the customer and verify his or her identity before establishing a business relationship or conducting a transaction. The laws nevertheless provide for limited circumstances where the verification may be differed:

### **Credit and Domestic Financial Institutions**

488. By way of derogation to the identification and verification requirements, a bank account may be opened provided that there are “adequate safeguards in place to ensure that transactions are not carried out by the customer or on the customer’s behalf” until full compliance with the identification requirements and the other information on the business relationship has been obtained (Article 40, paragraph 2c of the BWG). As an example of adequate safeguard, the authorities mentioned that this could be fulfilled by an IT-system that would automatically block any transaction [until] the financial institution has obtained all the relevant information on the business relationship and [until] fulfillment of all identification requirements.

### **Insurance Undertakings**

489. Insurance undertakings may differ the verification of the identity of the beneficiary under the insurance contract to a later stage (undefined in the law), but must complete the identification a verification process at the time of the payout, or when the beneficiary exercises the rights vested upon him or her under the insurance contract (Article 98b, paragraph 5 of the VAG).

### **Securities Institutions**

490. The WAG explicitly refers to the relevant provisions of the BWG for all AML/CFT preventive measures, including verification of the customer. The provisions described above therefore apply equally to the securities institutions. The authorities underscore that the provisions of Article 40, paragraph 2c of the BWG should apply rarely.

### ***Failure to Complete CDD before commencing the Business Relationship (c. 5.15) and after commencing the Business Relationship (c. 5.16)***

#### **Credit and Domestic Financial Institutions and Securities Institutions**

491. Pursuant to Article 40, paragraph 2d of the BWG, should the credit and domestic financial institutions and securities firms not be in a position to comply with the identification requirements set out under paragraphs 1, 2 and 2a of the same Article, they are prohibited from carrying out any transaction or establishing a business relations. They must also terminate ongoing business relationship and must consider filing a suspicious transaction report.

### **Insurance Undertakings**

492. The VAG provides for a similar prohibition under Article 98b, paragraph 6.

493. As a rule, financial institutions informed the assessors that they do not initiate any transaction before the CDD is completed.

### ***Existing Customers—CDD Requirements (c. 5.17):***

#### **Credit and Domestic Financial Institutions**

494. These institutions are required to identify existing customers “on a risk-sensitive basis at the appropriate time” (Article 40, paragraph 2e BWG). According to the authorities, a timeframe of one year after the entry in force (in January 2008) of the new provisions of the BWG is reasonable and allows credit and domestic financial institutions sufficient time to take measures. All institutions that have not complied with the requirement to identify existing customers by January 2009 will, therefore, be in violation of the law.

### **Insurance Undertakings**

495. Article 98b, paragraph 7 of the VAG reflects the substance of Article 40, paragraph 2e BWG within the insurance sector. According to the authorities, a timeframe of one year after the entry in force of the new requirement is deemed appropriate.

## **Securities Institutions**

496. The write-up on the credit and domestic financial institutions applies equally to the securities sector pursuant to Articles 6 and 12, paragraph 4 of the WAG.

497. During interviews, financial institutions mentioned different timeframes depending on the size of their customer base, some banks contemplating an extended period. No reference has been made to a prioritization of the process, based on a risk-adjusted approach.

### ***Existing Anonymous-account Customers—CDD Requirements (c. 5.18)***

498. According to the authorities, there are no anonymous banking accounts in Austria. For pre-existing anonymous savings accounts, amendments to the BWG, which came into effect on November 1, 2000, established special procedures which must be applied when customer's identity has not been ascertained yet:

- ascertain customer identity before receiving any deposit or allowing any withdrawal (Article 40, paragraph 7 of the BWG); and
- immediately inform the A-FIU of all withdrawal requests from a savings account which balance is equivalent to or above EUR 15,000 (Article 41, paragraph 1a of the BWG).

499. Savings deposits amounted to EUR 148.3 billion (as of June 30, 2008) and the estimated number of savings deposit accounts was 24.2 million. No global data was provided on the anonymous savings deposit accounts which are still in existence. The OeNB presented figures based on a review conducted at the end of 2007, on a sampling of 26 largest banks, representing 65 percent of total banking assets. Within this pool, 74 percent of the savings books' owners were identified, amounting to 98 percent of the total of savings book deposits. On this basis, it can be estimated that, in the country, 6.3 million accounts are not identified, amounting to EUR 2.97 billion, that is, an average balance for each savings book of EUR 472. Most of these savings deposits are considered as dormant accounts. The authorities indicated that a fee charged for closing a savings deposit account may act as a deterrent, notably when the deposited amount is lower than the fee.

### ***Foreign PEPs—Requirement to Identify (c. 6.1)***

## **Credit and Domestic Financial Institutions**

500. The BWG requires credit and domestic financial institutions to have appropriate risk-based procedures in place to determine whether a customer or the beneficial owner is a politically-exposed person from another country (PEP; Article 40b, paragraph 3). The law defines PEPs as natural persons who are (or were up to one year ago) entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons. In this context, "prominent public functions" refer to the following:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliaments;
- members of supreme courts, constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

- members of courts of auditors or of the boards of central banks;
- ambassadors, *chargés d'affaires* or high-ranking officers in the armed forces; and
- members of the administrative, management or supervisory bodies of state-owned enterprises.

With the exception of the last, all categories listed above also apply to positions at the European Community level and to positions in international organizations.

501. Are considered to be "immediate family members":

- spouses;
- partners who are considered equivalent to spouses under national law;
- children and their spouses or partners considered equivalent to spouses under national law; and
- parents.

502. The following are considered to be "persons known to be close associates":

- any natural person who is known to have joint beneficial ownership of a legal entity (such as a foundation) or of a trust with a person entrusted with a prominent public function, or who has other close business relations with a person entrusted with a prominent public function;
- any natural person who has sole beneficial ownership of a legal entity (such as a foundation) or of a trust which is known to have been set up de facto for the benefit of a person entrusted with a prominent public function.

503. The Austrian definition of PEPs does not include "important political party officials" which is listed as an example under the standard (see definition of PEPs in the FATF Glossary). The authorities maintained however that while not explicitly mentioned, most representatives of important political parties are nevertheless captured in the definition of PEPs due to their participation in either government or Parliament.

504. The BWG sets a one year timeframe from the end of the official functions after which a person is no longer considered a PEP. Beyond that timeframe, the general rule applies: enhanced due diligence measures are only mandatory if the credit or financial institutions consider that the ex-PEP still places them in a higher-risk situation.

505. There is no provision that addresses the fact that a customer may become a PEP in the course of a business relationship. Senior management approval is only required *before* the establishment of the business relationship with a PEP.

### **Insurance Undertakings and Securities Institutions**

506. Both the VAG and the WAG provide for similar definitions and requirements with respect to PEPs, the VAG by providing similar wording (Article 98d, paragraph 1, no. 2) and the WAG by

referring to the BWG (Articles 6 and 12, paragraph 4). The description made above, as well as the deficiency noted, apply equally with respect to insurance undertakings and securities firms.

***Foreign PEPs—Risk Management (c. 6.2; 6.2.1), Requirement to Determine Source of Wealth and Funds (c. 6.3) & Ongoing Monitoring (c. 6.4)***

**Banking Institutions**

507. Once a customer has been identified as a PEP, credit institutions and financial institutions must, in addition to applying standard CDD obligations:

- obtain senior management approval before establishing business relationships with such customers;
- take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction; and
- conduct enhanced ongoing monitoring of the business relationship (Article 40b, paragraph 1 no. 3, lit. b to d of the BWG).

**Insurance Undertakings**

508. Similar provisions are set out in Article 98d, paragraph 1, no. 2 of the VAG.

**Securities Institutions**

509. The provisions applicable to the credit and domestic financial institutions also applicable to investment firms and investment services companies (Articles 6 and 12, paragraph 4 of the WAG).

510. Former guidance published by the Banking Association recommended a detection of PEPs. Financial institutions the assessors visited have programs in place to detect PEPs, as well as approval procedures. However, it was not clear to the assessors the extent to which procedures have been defined to address other requirements of the standard as regards to determining the source of wealth and the source of funds and conducting enhanced monitoring.

***Domestic PEPs—Requirements (Additional Element c. 6.5)***

511. Domestic PEPs are not subject to enhanced due diligence measures: the BWG (to which the WAG refers) and the VAG clearly mention PEPs “from other [EU] Member States and from third countries.”

***Domestic PEPs—Ratification of the Merida Convention (Additional Element c. 6.6)***

512. Austria ratified the United Nations Convention against Corruption on January 11, 2006. In order to comply with the requirements of the Convention, Austria also amended its StGB by including new provisions on bribery which came into force on January 1, 2008. These new provisions criminalize bribery in the “private sector” (Articles 168c–168d), as well as in the “public sector” (Article 304). Pursuant to Articles 168c & 168d, accepting inappropriate gifts by employees or other authorized representatives of a (private) undertaking as well as bribery is forbidden by law. In the “public sector”, “office holders” (*Amtsträger*), arbitrators (*Schiedsrichter*), personnel of senior

management of public undertakings and expert advisors (*sachverständige Berater*) are addressees of the new provisions on bribery. “Office holders” are defined as all persons who hold an office for Austria, for any other country or for any international organization in the area of legislation, administration or adjudication or who are otherwise in charge of public duties, with the exception of parliamentarians (Article 74, paragraph 1 StGB). For parliamentarians, Article 304a, StGB sanctions bribery with regard to parliamentary votes or elections only.

513. Austria also volunteered to take part in a pilot program launched in 2007 with the aim to review the national implementation of the Convention. The result of the review was not shared with the assessors.

***Requirement to Obtain Information on Respondent Institution (c. 7.1), Assessment of AML/CFT Controls in Respondent Institution (c. 7.2), Approval of Establishing Correspondent Relationships (c. 7.3) & Documentation of AML/CFT Responsibilities for Each Institution (c. 7.4)***

514. Correspondent banking between Member States of the European Economic Area (EEA)<sup>28</sup> is not considered to be “cross-border.” The authorities justified this by the fact that, due to European community law, the EU and the EEA form a single market and all member States are subject to the same requirements. Only correspondent banking with “third countries”, that is, countries that do not belong to the EEA (Article 2, paragraph 8 of the BWG) is deemed to be of higher risk and is, therefore, subject to additional measures.

515. With respect to correspondent banking with non-EEA countries, Article 40b, paragraph 1, no. 2 of the BWG requires credit and domestic financial institutions:

- to gather sufficient information about a correspondent bank to understand fully the nature of its business and be able to ascertain the reputation of the institution and the quality of supervision on the basis of publicly available information;
- to satisfy themselves of the correspondent bank's anti-money laundering and anti-terrorist financing controls;
- to obtain approval from senior management before establishing new correspondent banking relationships;
- to document the respective responsibilities of each institution; and
- with respect to payable-through accounts, to satisfy themselves that the correspondent bank has verified the identity of and performed ongoing due diligence on the customers having

---

<sup>28</sup> The European Economic Area is an agreement between the members of the European Free Trade Association (EFTA), except Switzerland, the European Community (EC), and all Member States of the European Union (EU). It therefore comprises: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Liechtenstein, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

direct access to accounts of the correspondent, and that it is able to provide relevant customer due diligence data to the correspondent bank upon request.

***Payable-Through Accounts (c. 7.5)***

516. As mentioned above, credit and domestic financial institutions are also required to satisfy themselves that the correspondent bank that offers payable-through accounts has verified the identity of and performed ongoing due diligence on the customers that have direct access to the accounts of the correspondent, and that it is able to provide relevant due diligence data to the correspondent bank upon request (Article 40b, paragraph 1, no. 2 BWG).

**Effectiveness**

517. Most banks met during the assessment informed the assessors that they maintain a limited and selected number of correspondent accounts to which the new legal requirements would apply. In most cases, both the senior management and the management board have to give their approval to new correspondent relationships. Multinational institutions managing a larger network of correspondent banks exert a strict vigilance on the transactions they process, and suspicions have resulted in STRs be filed. The banks also mentioned that they do not offer payable through account facilities to their customers.

***Misuse of New Technology for ML/FT (c. 8.1)***

**All Financial Institutions**

518. There is no specific legal provision which requires financial institutions to define and implement policies and measures aiming at preventing the misuse of technological developments in money laundering or the financing of terrorism. The authorities consider however that such diligence falls within the ambit of the risk-based approach, and expect that financial institutions' risk analysis will result in classifying the misuse of new technologies in a high risk category, which require additional due diligence be taken on a risk-sensitive basis (Article 40b, paragraph 1 of the BWG, Article 98d, paragraph 1 of the VAG and Articles 6 and 12, paragraph 4, of the WAG referring to the BWG). Some of the new technology risks could be addressed under the specific requirements that apply to non-face-to-face transactions, but, altogether, the overall provisions fall short of fulfilling the conditions of criterion 8.1.

519. Financial institutions informed the assessors that internet services are the only new technology instruments they provide to their customers for accessing their account information and conducting secured transactions. According to them, in no circumstances can accounts be opened through the internet. At the time of the mission, none of the financial institutions the assessors met had included the misuse of technological developments in a high risk category.

***Risk of Non-Face-to-face Business Relationships (c. 8.2 & 8.2.1)***

**All Financial Institutions**

520. Article 40b, paragraph 1, no. 1 of the BWG, Article 98d, paragraph 1, no. 1 of the VAG, and Articles 6 and 12, paragraph 4 of the WAG, referring to the BWG, define non-face-to-face business

relationships as presenting a higher risk of ML/FT requiring that mandatory enhanced due diligence be applied on a risk-sensitive basis to ascertaining and verifying the identity of a customer.

521. The minimum requirements are that:

1. An electronic signature or registered mail is used;
2. Identification data are known to the financial institution; the customer confirms in writing that the place of incorporation of a legal person is also the seat of its central administration; a copy of the identification documents is obtained; and
3. When the customer resides or is incorporated outside the EEA, a written declaration is obtained from a credit institution with which the customer has a permanent business relationship stating that the identification procedure has been completed in a manner which is in accordance with Austrian rules, or when the credit institution is incorporated in a third country, consistent with Articles 16-18 of the Directive 2005/60/EC, and that the business relationship is still maintained (identification and confirmation by the Austrian representation on the third country or a recognized certification authority is also permissible).

Or

1. The first payment is carried out through an account opened in the customer's name with a credit institution situated in an EU Member State or a third country having an AML/CFT regime consistent with the EU rules; the customer identification data, whether natural or legal person, must be known to the financial institution.
2. Financial institutions must either have the documents required to verify customer's identity, or obtain a written declaration from the credit institution through which the payment is made stating that the customer has been identified in accordance with Austrian rules or Article 8(1) (a) to (c) of Directive 2005/60/EC.

522. For insurance undertakings, the above-mentioned requirements are waived for life insurance contracts where the annual premium is below EUR 1,000 or the single premium is lower than EUR 2,500, and which are considered as presenting low ML/FT risks (Article 98d, paragraph 1, no. 1 in fine of the VAG). Notwithstanding, business relations must be avoided in cases of suspicion or reasonable grounds for suspicion of money laundering or financing of terrorism.

523. The BWG, VAG and WAG set minimum mandatory diligence for customer identification and verification when initiating non-face-to-face business relationships. Financial institutions are not required to have specific policies and procedures in place to address any related risk, but non-face-to-face transactions are recognized as a higher risk of ML/FT, mandating financial institutions to apply additional due diligence measures on a risk-sensitive basis.

524. During meetings, some financial institutions reported that non-face-to-face business was subject to enhanced scrutiny. The assessors were informed that non-face-to-face business relationships and transactions were limited to activity intermediated by agents and brokers. The former operate as financial institutions' commercial staff, as described in Recommendation 5, and the latter fall under the provisions for intermediaries, analyzed in Recommendation 9.

### 3.2.2 Recommendations and Comments

525. Overall, the measures set out in the BWG, VAG and WAG are broadly in line with the standard in their substance. They nevertheless suffer from a number of shortcomings and, in most cases, their effectiveness has not been established. For instance, the blanket exemptions from performing CDD measures and from conducting additional measures with respect to cross-border correspondence banking fall short of the standard. The Austrian authorities implicitly assume that the level of compliance with the standard is effective and adequate throughout the EU and the EEA membership without having performed a risk assessment that would establish whether an exemption is justified. The fact that all EU members are subject to the same requirements does not necessarily entail adequate implementation throughout the membership. More generally, there is no evidence of a risk assessment of the overall financial sector. This is evident with respect to certain types of businesses, such as private banking for example, which are frequent in Austria and are generally accepted as justifying enhanced due diligence measures but where the additional risk has not been mitigated in Austria by adequate CDD obligations.

526. Although the revision of the AML/CFT legal framework came into force on January 1, 2008, several of the FMA's operational circulars are still pending, and should be completed in the forthcoming months. The new requirements (PEPs, correspondent accounts, beneficial ownership) are still at too early a stage of implementation by the industry to be evaluated for their effectiveness.

527. The timeframe that applies to the definition of PEPs in accordance with the BWG entails that former PEPs are no longer subject to enhanced due diligence measures after a period of one year from the end of their official functions. The standard clearly covers those "who are or *have been* entrusted with public functions", and does not include a limit in time. However, the one-year timeframe appears reasonable in the Austrian context given the obligation to apply enhanced due diligence in case of higher risk: If a former PEP still presents a higher risk more than one year after leaving office, enhanced due diligence must be applied. Unlike the standard, the Austrian legislation does not address the possibility of a customer becoming a PEP during the course of the business relationship and is quite clear in requiring management approval for establishing a business relationship with a PEP, not for continuing a relationship with an existing customer who subsequently becomes a PEP.

528. Recommendation 8 sets out various obligations to prevent technological and non-face-to-face risks which must be defined in law, regulation or other enforceable means. Addressing the requirement to have policies and procedures to prevent the misuse of technological developments is left to financial institutions which are supposed to classify technological developments in higher risk categories. Conversely, the Austrian regime establishes specific additional identification and verification diligence at the inception of non-face-to-face business relationships which are listed as higher risks, triggering the application of additional due diligence on a risk-sensitive basis.

529. In light of the above, the authorities should:

#### Recommendation 5

- Require that holders of savings documents for savings deposit accounts which balance is lower than EUR 15,000 and are not registered in the customer's name, be considered as beneficial owners and be subject to corresponding identification and verification obligations;

- Extend CDD measures to customers that are credit and financial institutions established in EU member countries;
- Remove the blanket exemption for fiduciary accounts below EUR 15,000;
- Conduct domestic ML/FT risk assessment and require enhanced due diligence measures with respect to business relationships and transactions that are of higher risk;
- Issue guidelines on the extent of the CDD measures on a risk sensitive basis;
- Consider requiring banks to remove the fee charged for closing a savings deposit account.

#### **Recommendation 6**

- Request financial institutions to apply enhanced due diligence when a customer becomes a PEP after the establishment of the business relationship.

#### **Recommendation 7**

- Apply the measures listed under Article 40b, paragraph 1, no. 2 of the BWG to all correspondent banking, that is, also with respect to EEA Member States.

#### **Recommendation 8**

- Require financial institutions to have policies in place or to take measures to prevent the misuse of technological developments in ML/FT schemes.

### **3.2.3 Compliance with Recommendations 5 to 8**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R.5</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Undue exemption from CDD measures for customers that are credit institutions established in EU member countries.</li> <li>• Undue blanket exemption from CDD measures for fiduciary accounts that amount to less than EUR 15,000.</li> <li>• No requirement to apply beneficial owner's identification and verification diligence to holders of savings documents for savings deposit accounts which balance is lower than EUR 15,000 and are not registered in the customer's name.</li> <li>• Current list of suggested high-risk customers omits some significant high risk business categories relevant to Austria.</li> <li>• No guidelines issued by the competent authorities on the extent of the CDD measures on a risk sensitive basis.</li> <li>• Effectiveness was not established for some criteria.</li> </ul>
<b>R.6</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Measures in place limited to customers who fit the definition of a PEP at the</li> </ul>

		beginning of a business relationship only. <ul style="list-style-type: none"> <li>Effectiveness not established.</li> </ul>
<b>R.7</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>Undue exemption from additional measures for correspondent relationships with credit institutions established in EEA member countries.</li> </ul>
<b>R.8</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>No requirement for financial institutions to have policies in place or to take measures to prevent the misuse of technological developments in ML/FT schemes.</li> </ul>

### 3.3 Third Parties And Introduced Business (R.9)

#### 3.3.1 Description and Analysis

##### Legal Framework

##### *All Financial Institutions*

530. Provisions in the BWG (Article 40, paragraph 8) and the VAG (Article 98e) set conditions for financial institutions wishing to rely on third parties to meet their obligations to identify and verify customers and beneficial owners, and to collect information on the purpose and nature of the intended business relationship. Articles 6 and 12, paragraph 4 of the WAG carry over the provisions of the BWG. The following are considered third parties:

- credit institutions and financial institutions, as defined in Article 3, paragraphs 1 and 2 of Directive 2005/60/EC, notably life insurance companies and insurance intermediaries, investment firms, collective investment undertakings marketing their units or shares (institutions carrying out exclusively exchange bureau or money remittance services business are explicitly excluded); and
- auditors, external accountants, tax advisors, notaries and legal professions, as defined in Article 2, paragraphs 1 and 3a, and b of Directive 2005/60/EC.

531. Such professionals must be subject to mandatory professional registration recognized by law, must apply the CDD and record keeping requirements set out in the Austrian law or the EU Directive and are subject to AML/CFT supervision as set forth in the Third EU ML Directive. Third parties can only be located in a non-EU country which applies equivalent AML/CFT provisions and supervision.

532. In the Austrian system, insurance intermediaries are subject to the AML/CFT provisions of the Trade Act (*Gewerbeordnung, GewO*), and are also supervised for compliance with those provisions by the local district authorities (*Bezirksverwaltungsbehörden*).

##### ***Requirement to Immediately Obtain Certain CDD elements from Third Parties (c. 9.1); Availability of Identification Data from Third Parties (c. 9.2)***

533. Financial institutions must ensure that the third parties make CDD information available to them without delay and that relevant copies of CDD data and documentation are immediately

forwarded on their request (Article 40, paragraph 8 of the BWG and Article 98e, paragraph 4 of the VAG).

***Regulation and Supervision of Third Party (c. 9.3, applying R. 23, 24 & 29) & Adequacy of Application of FATF Recommendations (c. 9.4)***

534. In accordance to the BWG (Article 40, paragraph 8) and the VAG (Article 98e), financial institutions may only rely on third parties which are subject to AML/CFT requirements and supervision as set forth in Directive 2005/60/EC, or are situated in countries which AML/CFT requirements and supervision are equivalent to those of the Directive. The FMA must inform other EU Member States and the EU Commission when it considers that a third country does not meet the requirements above (Article 40, paragraph 8 of the BWG). Until now, no country has been reported by the FMA. The Austrian authorities implicitly assume that the level of compliance with the standard is effective and adequate throughout the EU and the EEA membership without having performed a risk assessment that would establish whether an exemption is justified. The fact that all EU members are subject to the same requirements does not necessarily entail adequate implementation throughout the membership. The FMA has transmitted the EU list of “third countries” (i.e., non-EU countries) which are considered as having an equivalent AML/CFT regime to financial institutions with no modification.

***Ultimate Responsibility for CDD (c. 9.5)***

535. The ultimate responsibility for meeting the legal obligations remains with the financial institution relying on third parties (Article 40, paragraph 8 of the BWG, Article 98e paragraph 1 of the VAG).

**Effectiveness**

536. During interviews with the private sector, the assessors were told that securities institutions and insurance undertakings use intermediaries to enter into new business relationships. Intermediaries operate under the procedures of financial institutions, and collect on their behalf all information required to build a customer profile (in the securities business, similar information are required by MIFID). Financial institutions made a distinction between the application process, conducted by the third party when visiting the customer, and the customer acceptance process which always remains with the financial institution. However, financial institutions, which do not have a face-to-face contact with the client, rely on the identification diligence conducted by the intermediary. In many situations, they would not have a photocopy of the identification document, but only an indication of the type of identification document presented to the third party. Contract processing typically requires that acceptance documents be mailed to the client, and funds must always be processed through an account in the customer name at a bank located in Austria. Some insurance firms consider business through intermediaries as a higher risk that they will enter as a risk factor in the transaction monitoring systems they are developing, in accordance with the new legal provisions. Some institutions provide training to their agents, but not to brokers.

### 3.3.2 Recommendations and Comments

537. The authorities should determine whether EU and EEA countries where third parties are based adequately apply the FATF Recommendations.

### 3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
<b>R.9</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Presumption that all EU and EEA countries adequately apply the FATF recommendations.</li> </ul>

## 3.4 Financial Institution Secrecy or Confidentiality (R.4)

### 3.4.1 Description and Analysis

#### *Inhibition of Implementation of FATF Recommendations (c. 4.1)*

#### **Credit and Domestic Financial Institutions**

538. The banking secrecy requirement is set out in Article 38, paragraph 1 of the BWG as follows: credit institutions, their members, members of their governing bodies, their employees as well as any other persons acting on behalf of credit institutions are prohibited from divulging or exploiting secrets which are revealed or made accessible to them exclusively on the basis of business relations with customers, or on the basis of Article 75, paragraph 3 (banking secrecy). The secrecy requirement extends to the functionaries of authorities as well as the OeNB that acquire knowledge subject to banking secrecy requirements in the course of their duties. The obligation to maintain secrecy applies for an indefinite period of time. The provision on banking secrecy may only be amended by the National Council with at least one half of the representatives present and a two third majority of the votes cast (Article 38, paragraph 5).

539. Anyone who discloses or exploits facts subject to the banking secrecy in order to create an economical advantage for himself or for others, or in order to place others at a disadvantage, is punishable by the courts to imprisonment for up to one year or with a fine of up to 360 days-fine<sup>29</sup> (Article 101, paragraph 1 of the BWG). The offender may only be prosecuted with the authorization of the person whose interest in secrecy was violated (Article 101, paragraph 2 of the BWG).

540. Access to information usually covered by the banking secrecy is nevertheless possible pursuant to the provisions set out in the BWG and the StPO:

<sup>29</sup> Pursuant to Article 19 of the StGB, monetary fines are to be pronounced in daily rates. The minimum fine is two daily rates. The daily rate is to be laid down according to the personal and economic situation of the perpetrator at the time of the verdict of the court of the first instance. The daily rates range between a minimum of EUR 2 and a maximum of EUR 500. A substitute prison sentence is to be pronounced if the fine cannot be executed. One day of substitute prison sentence is equivalent to two daily rates.

541. Article 38, paragraph 2 of the BWG explicitly provides a list of circumstances where the banking secrecy does not apply, that is:

- vis-à-vis public prosecutors and criminal courts in connection with criminal court proceedings on the basis of a court approval (Article 116 StPO), and vis-à-vis the fiscal authorities in connection with initiated criminal proceedings due to willful fiscal offenses, except in the case of financial misdemeanors;
- in the case of obligations to provide information such as the obligation to report suspicions of money laundering or terrorist financing and the obligation to provide the Police with all relevant information, as set out in Article 41, paragraphs 1 and 2;
- vis-à-vis the probate court and the court commissioner in the event of the death of a customer;
- vis-à-vis the competent court for guardianship or tutelage matters if the customer is a minor or otherwise under tutelage;
- if the customer grants his/her express written consent to the disclosure of secrets;
- for general information commonly provided in the banking business on the economic situation of an undertaking, unless the undertaking expressly objects to the provision of such information;
- where disclosure is necessary in order to resolve legal matters arising from the relationship between the credit institution and customer;
- with regard to the reporting requirements pursuant to Article 25, paragraph 1 of the Inheritance and Gift Tax Act (*Erbschafts- und Schenkungssteuergesetz*); and
- in the case of obligations to provide information to the FMA pursuant to the Securities Supervision Act and the Stock Exchange Act.

542. The authorities pointed out that the catalogue of exemptions to the banking secrecy requirement set out in Article 38, paragraph 2 BWG is not exhaustive according to the case law of the High Administrative Court and the Supreme Court of Justice, as well as to Austrian expert literature.<sup>30</sup> With respect to AML/FT matters, the authorities maintain that further implicit exceptions are recognized on the basis of the following provisions:

- According to Article 78 StGB, the FMA (as any other public authority) is obliged to report the suspicion of a crime to the public prosecution or criminal police. To comply with this obligation, it is allowed to provide information or documents underlying banking secrecy;
- The FMA is obliged to report the suspect of misuse of insider-information to public prosecution according to Article 48i of the BörseG. In these circumstances too, the FMA is allowed to provide information/documents underlying banking secrecy to comply with this obligation;

---

<sup>30</sup> VwGH 94/17/0297; OGH ÖBA 1988, 1022 Laurer in Fremuth/Laurer/Linc/ Pötzelberger/Strobl, Bankwesengesetz, 2. Auflage, Rz 10ff zu Article 38 BWG

- The public prosecution may mandate the FMA with further investigations on the suspicion of misuse of insider-information. The FMA has to report any information and results and provide all documents obtained; and
- Pursuant to Article 41, paragraph 5 of the BWG, if the FMA or the National Bank, in performing their supervisory duties, find reason to suspect that a transaction serves the purpose of ML/FT they must file a report to the A-FIU without delay. To comply with this obligation, both authorities are allowed to provide information/documents underlying banking secrecy.

543. The legal basis for obtaining relevant ML/FT information and documents is provided by Article 41, paragraph 2 of the BWG which states that “Upon request, credit institutions and financial institutions must provide the authority with all information which the authority deems necessary in order to prevent or pursue cases of money laundering or terrorist financing.” Such disclosure of information is explicitly exempt from the obligation to obey banking secrecy (Article 38, paragraph 2, no. 2 BWG).

544. Two types of information are considered for disclosure under Article 109 of the StPO and different conditions are set out for their disclosure. “Information on bank accounts and bank operations” are defined in Article 109, paragraph 3 of the StPO as:

- a) [...] the name and other information about the identity of the holder of a business relation as well as his/her address and the information whether an accused person maintains business relations with this institution, is entitled to economic advantages from this relation or authorized by such relation as well as the presentation of all documents regarding the identity of the holder of the business relation and his authorization to act; and
- b) [...] documents and other papers of a credit or financial institution regarding the nature and extend of a business relation and other business operations for a determined past or future period of time.

545. Access to the information defined under Article 109, Paragraph 3, lit. a (i.e., mainly the name and address) is admitted if it seems to be necessary to clarify a felony/criminal offense or misdemeanor that falls within the jurisdiction of the Provincial Court (Article 17 of the StGB in conjunction with Article 31, paragraphs 2-4 of the StPO). However, access to the information listed under 109, paragraph 3, lit. b (such as extracts of a bank account for example) is only admitted by Article 116, paragraph 2 of the StPO: “if due to particular circumstances<sup>31</sup> it can be assumed that:

1. The business relation of a person with the credit or financial institution is connected to committing a criminal act and either the holder of the account himself/herself is suspected of having committed the act or if it is presumed that a person suspected of

---

<sup>31</sup> The official English translation of Article 116, paragraph 2 of the StPO is misleading according to the authorities: the correct translation of “auf Grund bestimmte Grundsachen” should be “due to particular circumstances” and not “on the basis of ascertained facts..” For the purposes of this assessment, the assessors used the translation referred to by the authorities, i.e., “due to particular circumstances..”

having committed the act will operate or has operated a transaction via the account,  
or

2. The business relation will be used for the transaction of a financial benefit that was gained through criminal acts or gained for them (Section 20 of the StGB) or is subject to the disposition of a criminal organization or terrorist organization or is provided or collected as a means of financing terrorism (Section 20b of the StGB).”

546. The disclosure of information on bank accounts and bank operations must be requested by the office of public prosecution and ordered by the court (Article 116, paragraph 3 of the StPO). The public prosecutor’s request and the court order must contain the following information:

- the denomination of the court case and the criminal act it is based on as well as its legal denomination;
- the credit or financial institution;
- the designation of the documents to be handed over and the information to be disclosed;
- the facts that constitute the grounds for the necessity and proportionality (section 5) of the order;
- in the case of an order according to paragraph 2 the time frame concerning which the operations are to be disclosed; and
- in the case of an order according to paragraph 2 the facts that constitute the grounds for the connection between the business relation and the subject of the proceeding.

547. Both the request and the court order must be served to the credit or financial institution, the accused and the persons entitled by the business relation, as soon as they are known to the office of public prosecution. Service to the accused and to the entitled persons can be postponed as long as otherwise the aim of the proceeding would be endangered. The credit or financial institution has to be informed of this and has to keep the order and all facts and operations in connection with it secret against clients and third parties (Article 116, paragraph 5 of the StPO).

548. Article 116, paragraph 5 of the StPO also provides that credit and domestic financial institutions and their employees are obliged to disclose the requested information, to let the documents and papers be inspected and hand them over. In case more information is needed or more documents are to be provided for inspection or to be handed over, that are not included in the request and the court order (paragraph 4), a procedure according to Article 112 is to be initialized if the credit or financial institution requests it.

### **Insurance Companies**

549. While Article 108a of the VAG sanctions the violation of the duty of secrecy in the insurance business, the duty of secrecy is in fact much weaker than the banking secrecy. Indeed, Article 108a VAG does not apply “if the disclosure or use is justified as to content and form by a public or a legitimate private interest.” Disclosure is granted where it is justified by a “*public interest*”, which is always the case in criminal investigation. Outside criminal proceedings: The FMA and the OeNB

may require any information when performing their functions, but access to the information in other circumstances is only possible through the A-FIU (Article 98e, paragraph 3 of the VAG).

### **Effectiveness**

550. Financial institutions have frequent informal exchanges with the A-FIU on AML/CFT-related issues, which may result in filing a STR. Investigations by other police units must be presented in the form of a court order. Some institutions told the assessors that they decline those requests which do not provide enough evidence that the legal conditions to lifting banking secrecy are material and adequate. Discussions with the authorities and with representatives of the banking industry indicated that the credit and domestic financial institutions usually comply with all requests emanating from the police acting on the basis of an STR, but are more reluctant to follow court orders and refuse to execute the order when they consider that the link between the client or the transaction and the suspicions of money laundering or terrorist financing has not been clearly established.

551. The supervisory authority does not appear to encounter difficulties in obtaining the information it needs to fulfill its obligations.

### **3.4.2 Recommendations and Comments**

552. Overall, the provisions set out in the BWG and the StPO seem to enable the authorities to access the information they require in order to exercise their functions in the fight against money laundering and terrorist financing. In practice however, access to the information covered by the banking secrecy raises difficulties when it is required in the course of criminal proceedings: while the access to the banking records by the police/A-FIU acting on the basis of Article 38, paragraph 2 second bullet point of the BWG is unproblematic (the police must only indicate that there is a suspicion of money laundering or terrorist financing), the access in other circumstances is more difficult. As mentioned under the write-up on confiscation, the conditions to be fulfilled in order to obtain a court order for the disclosure of banking information under Article 116 of the StPO are quite restrictive, in particular when the information sought goes beyond the mere name and address of the customer. In the request for the court order, the prosecutor must show on the basis of “particular circumstances” that (i) the business relationship between a person and the credit or financial institution is “connected to committing a criminal act”, and (ii) that “either the holder of the account himself/herself is suspected of having committed the act or it is presumed that a person suspected of having committed the act will operate or has operated a transaction via the account”, or that “the business relation will be used for the transaction of a financial benefit that was gained through criminal acts or gained for them or is subject to the disposition of a criminal organization or terrorist group or is provided or collected as a means of financing terrorism. The police and the prosecution must therefore be in possession of a fair amount of information before they may even consider applying for a court order for the disclosure of banking records. Unless the link to an offense is clear from the start, access to banking records would therefore appear to be impossible in the early stages of the investigative process.

553. Discussions with the authorities and with representatives of the banking industry indicated that the credit and domestic financial institutions usually comply with all requests emanating from the police acting on the basis of the BWG, but are more reluctant to follow court orders and refuse to execute the order when they consider that the link between the client or the transaction and the

suspicions of money laundering or terrorist financing has not been clearly established. In other words, the credit and domestic financial institutions substitute their own appreciation of a specific case to that of the court, thus “forcing” the latter to reconsider the case and re-establish the link with a money laundering or terrorist financing crime.

554. The authorities should lighten the conditions set out in Article 116 of the StPO for disclosure of banking information in order to facilitate access by the police to banking records.

### 3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	PC	<ul style="list-style-type: none"> <li>Disclosure of banking information under Article 116, paragraph 3, lit. b StPO is subject to restrictive conditions which hamper access to relevant information in practice.</li> </ul>

## 3.5 Record-Keeping and Wire Transfer Rules (R.10 & SR.VII)

### 3.5.1 Description and Analysis

#### Legal Framework

555. The legal provisions applicable to the retention of relevant information and wire transfers are set out respectively in the sector-specific laws (BWG, VAG and WAG) and in the EU Regulation (EC) No. 1781/2006.

#### *Record-Keeping & Reconstruction of Transaction Records (c. 10.1 & 10.1.1) & Record-Keeping for Identification Data, Files and Correspondence (c. 10.2)*

#### Credit and Domestic Financial Institutions

556. Credit and domestic financial institutions are required by law to retain:

- identification documents for at least five years after the termination of the business relationship; and
- documentation and records of all transactions for a period of at least five years after their execution (Article 40, paragraph 3 of the BWG). This last requirement applies regardless of whether the transactions were domestic or international.

557. The law ensures that all necessary documents necessary to reconstruct a specific customer relationship or transactions are maintained for at least five years.

558. The relevant authorities may request the information and documents in the course of an investigation following the filing of an STR under Article 41, paragraph 2 of the BWG, and in other criminal proceedings under Article 38, paragraph 2 of the same law. The FMA and the OeNB may access the information in the exercise of their supervisory functions. The authorities indicate that Article 212, paragraph 1 of the Commercial Code (UGB) require that entrepreneurs preserve an extensive list of commercial documents for seven years, or longer if relevant for pending court or

administrative proceedings. They underscore that, in practice, data are stored in electronic format which allows extended record keeping duration.

### ***Insurance Undertakings***

559. Article 98g of the VAG provides that insurance undertakings must retain the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the A-FIU or the FMA:

- any and all identification documents as well as supporting evidence and records of insurance contract for at least five years following the termination of the insurance contract;
- the supporting evidence and records for a period of at least five years following the carrying out of the transactions.

560. The wording of the law ensures that the A-FIU and the FMA may have access to sufficient information of individual contracts and transactions. However, it does not enable the authorities to request a longer record retention period if necessary.

### ***Securities Institutions***

561. The WAG requires investment institutions and investment services companies to follow the record keeping set forth in the BWG and described above (Articles 6 and 12, paragraph 4).

### ***Availability of Records to Competent Authorities in a Timely Manner (c. 10.3)***

562. Financial institutions are required to provide the A-FIU with all information it requests in order to prevent or prosecute ML or FT (Article 41, paragraph 2 of the BWG, Article 98f, paragraph 2 of the VAG, and Articles 6 and 12, paragraph 4 of the WAG, applying Article 41 BWG. The requirement to respond fully and rapidly exists for A-FIU or FMA inquiries about ML/FT cases as to whether financial institutions maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship (Article 41, paragraph 4, no. 4 of the BWG, Article 98h, paragraph 1, no. 4 of the VAG, and Articles 6 and 12, paragraph 4 of the WAG applying Article 41 BWG). In the authorities' view, the nature of the relationship means all customer and transaction records and information. Neither the A-FIU, nor the FMA have mentioned excessive delays in obtaining all relevant data and information from financial institutions.

### ***Special Recommendation VII—Wire Transfers***

563. Requirements under SR.VII have been implemented within the EU through Regulation (EC) No. 1781/2006, in force since January 1, 2007. This Regulation lays down the same law throughout the European Union, regardless of borders and applies in full in all Member States, including Austria. Member States are not allowed to set up provisions or practices of domestic law that would preclude the mandatory application of the regulation. EU Regulations are directly applicable throughout the EU membership. They confer rights or impose obligations on the EU citizens in the same way as national law. The Member States and their governing institutions are bound directly by the regulation and have to comply with it in the same way as with national law. National implementation is therefore limited to establishing an appropriate monitoring, enforcement and penalties regime and to

applying certain derogations allowed for in the Regulation. Requirements applicable by credit institutions with respect to wire transfers are therefore set out in the EU Regulation.

564. The EU Regulation applies to transfers of funds, in any currency, which are sent or received by a payment service provider established in the EU, except in the following circumstances:

- transfers of funds carried out using a credit or debit card under specific conditions (Article 3, paragraph 2), electronic money up to a threshold of EUR 1,000 (Article 3(3));
- transfer of funds carried out by means of a mobile phone or similar device (Article 3, paragraphs 4 and 5);
- cash withdrawals, transfers related to certain debit transfer authorizations, truncated cheques, transfers to public authorities for taxes, fines or other levies within a Member State;
- transfers where both the payer and the payee are payment service providers acting on their own behalf (Article 3, paragraph 7).

***Obtain Originator Information for Wire Transfers (applying c. 5.2 & 5.3 in R.5, c.VII.1)***

565. Articles 4 and 5 of the EU Regulation EC No. 1781/2006 requires credit institutions to ensure that all transfers are accompanied by “complete information” on the originator, that is:

- the name of the originator;
- the originator’s account number; and
- the originator’s address.

566. The originator’s credit institution must verify the full originator information on the basis of documents, data or information obtained from a reliable and independent source before executing a wire transfer, regardless of any threshold (Article 5, paragraph 2 of the EU Regulation). Pursuant to Article 40, paragraph 1 of the BWG, the identity of the customer must be verified against an official identification documents as described in the write-up on Recommendation 5 above.

567. The EU Regulation also provides for exceptions to the verification requirements when the transfer is executed from an account:

- of a customer who has been identified in the course of the account opening and whose identification records have been stored according to the requirements described under criterion 5.3 above;
- of an existing customer whose identify has to be verified at an appropriate time as described under the same criterion (Article 5, paragraph 3 of the EU Regulation)

568. When transfers are no made from a an account, the financial institution must verify the identity of the originator of transactions above EUR 1,000, in case of or several transactions of a lower amount but which appear to be linked and together exceed EUR 1,000 (Article 5, paragraph 4 of the EU Regulation).

***Inclusion of Originator Information in Cross-Border Wire Transfers (c. VII.2)***

569. In line with the changes made to the criterion VII. 3 of the methodology in June 2008, transfers between Austria and another EU member country are considered as domestic for the purposes of this assessment, while transfers between Austria and non-EU member states are considered as cross-border.

570. Pursuant to Article 7, paragraph 1 of the EU Regulation, wire transfers from the EU to non-EU countries must be accompanied by full originator information. In case of batch transfers, however, it is not necessary that each individual wire transfer be accompanied by the full originator information provided that the batch file contains the necessary information and that the originator's account number (or unique identifier) is attached to each individual wire transfer (Article 7, paragraph 2 of the EU Regulation).

### ***Inclusion of Originator Information in Domestic Wire Transfers (c. VII.3)***

571. Wire transfers between Austria and other EU member countries need not be accompanied by full originator information and may only contain the account number or a unique identifier allowing the transaction to be traced back to the originator (Article 6(1) of Regulation (EC) No. 1781/2006).

572. However, if requested by the financial institution of the beneficiary, the financial institution of the originator must nevertheless make the full originator information available within three working days (Article 6(2) of Regulation (EC) No. 1781/2006).

573. Both the financial institution of the originator and of the beneficiary are required to respond fully and without delay to requests made by competent authorities (Article 14 of Regulation (EC) No. 1781/2006).

### ***Maintenance of Originator Information (c. VII.4)***

574. Pursuant to Article 12 of the EU Regulation, the intermediary financial institution must ensure that all originator information received is kept with the transfer. Beneficiary financial institutions are required to verify whether information on the originator is missing or incomplete and must therefore ensure that originator information has been transmitted with the wire transfer (Article 8 of Regulation (EC) No. 1781/2006).

575. In the case of technical limitations to a payment system, intermediary financial institutions must keep records of all originator information received for five years (Article 13, paragraphs 2 and 5 of Regulation (EC) No. 1781/2006).

### ***Risk-Based Procedures for Transfers Not Accompanied by Originator Information (c. VII.5)***

576. Article 8 of Regulation (EC) No. 1781/2006 sets out the obligations for the beneficiary financial institution to detect whether the fields within the messaging or payment and settlement system used for a transfer of funds concerning the information on the originator have been completed according to the characters or inputs admissible within the conventions of that system. For this purpose, the financial institution of the beneficiary must have effective procedures in place to detect any missing element in the required originator information.

577. If the financial institution of the beneficiary becomes aware that required information on the originator is missing or incomplete, it has to either reject the transfer or request full originator information. If a financial institution regularly fails to supply the originator information required under the Regulation, the beneficiary financial institution is required to take steps (from issuing warnings and setting deadlines, rejecting any future wire transfers from the specific financial institution up to restricting or terminating its business relationship) and to report this fact to the competent authorities (Article 9 of Regulation (EC) No. 1781/2006).

578. Additionally, Article 10 of EU Regulation requires the beneficiary financial institution to consider missing or incomplete originator information as a factor in assessing whether the wire transfer is suspicious and whether it must be reported according to the obligations set out under the Third EU ML Directive (implemented through Article 41, paragraph 1 BWG).

***Monitoring of Implementation (c. VII.6) & Application of Sanctions (c. VII.7: applying c.17.1 – 17.4)***

579. Article 15 of the EU Regulation obliges Austria to lay down rules on penalties in case of infringements of the provisions of the Regulation and to ensure that competent authorities monitor and take necessary measures with a view to ensuring compliance with the Regulation.

580. The competent authority monitoring and enforcing compliance with the requirements of Regulation (EC) No. 1781/2006 is the FMA. Financial institutions failing to comply with the requirements set out under the Regulation are guilty of an administrative offense and are to be punished with a fine up to EUR 30,000 (Article 99, no. 19 BWG).

581. The FMA assesses this recommendation in the course of its usual supervisory procedures. At the time of the assessment, no practical failure to comply with the relevant requirements had been detected.

***Additional Elements: Elimination of Thresholds (c. VII.8 and c. VII.9) (c. VII.8 and c. VII.9)***

582. Regarding incoming cross-border transfers, Article 8(b) of Regulation (EC) No. 1781/2006 requires financial institutions of the beneficiary to detect whether wire transfers where the financial institution of the originator is situated outside the EU are accompanied by full originator information or not. If not, the financial institution of the beneficiary has to comply with the obligations described above (and the exemptions for batch files mentioned above are applicable) regardless of any thresholds.

583. Concerning outgoing cross-border transfers, Article 7 of the EU Regulation requires that any wire transfer where the financial institution of the beneficiary is situated outside the EU has to be accompanied by full originator information, regardless of any threshold. (The exemptions for batch files described above are also applicable.)

**3.5.2 Recommendations and Comments**

584. Recommendation 10 and Special Recommendation VII are fully observed.

### 3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
<b>R.10</b>	C	
<b>SR.VII</b>	C	

## 3.6 Monitoring of Transactions and Relationships (R.11 & 21)

### 3.6.1 Description and Analysis

#### *Special Attention to Complex, Unusual Large Transactions (c. 11.1)*

585. Credit and domestic financial institutions, as well as securities institutions, are required to “pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing, in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose”, and to keep suitable records on these activities (Article 41, paragraph 1 of the BWG, and Articles 6 and 12, paragraph 4 of the WAG, referring to the BWG).

586. For insurance undertakings, the requirement is formulated in Article 98f, paragraph 1 of the VAG: “in particular complex or unusual contract terms and transactions which have no apparent economic or visible lawful purpose.” It shows a divergence from the standard, since it does not include “unusual patterns of transactions”, and would not typically include situations where series of transactions or contracts could raise suspicions, while each of them considered in isolation would not be suspicious.

#### *Examination of Complex & Unusual Transactions (c. 11.2)*

587. Laws require financial institutions only to pay special attention to these activities and to keep suitable records on such activities. Additionally, the authorities point to the provisions related to the risk-based approach:

- Article 40, paragraph 2b of the BWG and Article 94b, paragraph 4 of the VAG require financial institutions to subject their business to risk analysis using suitable criteria with regard to the ML/FT risks and to be able to demonstrate to the FMA that the measures taken on the basis of the analysis is appropriate; and
- Article 40b, paragraph 2 of the BWG -and Articles 6 and 12, paragraph 4 of the WAG, referring to the BWG- and Article 98d, paragraph 2 of the VAG, stipulate that credit institutions and domestic financial institutions must review with particular care transactions that they regard as particularly likely, by their nature, to be related to ML/FT.

588. While valuable, these provisions do not fully address the requirement defined by the standard. The former refer to ML/FT risks arising from the business, not from transactions; the latter defines a similar obligation (review suspicious transactions with particular care). However, the nature and

extent of diligence required to perform transaction monitoring are left to financial institutions, and may not include the examination of the background and purpose of such transactions, as required in c.11.2.

***Record-Keeping of Findings of Examination (c. 11.3)***

589. Article 41, paragraph 1 of the BWG and Article 98f, paragraph 1 of the VAG requires that “suitable records” be kept for transactions to which special attention has been paid. There is no obligation for financial institutions to keep them for at least five years. As there is no definition in law, regulation or other enforceable means of the diligence required, it is not clear what suitable records would be. It is possible that general provisions for record keeping (see section 3.5) would apply for identification documents, and documentation and records of transactions. However, these provisions would not include investigating documentation relating to complex, unusual large transactions or pattern of transactions as well.

**Effectiveness**

590. The 2007 revision of BWG, VAG and WAG, effective since January 1 2008, introduced the requirement to pay special attention to any activity which financial institutions regard as likely to be related to money laundering or financing of terrorism. Apart from internationally active banks, financial institutions generally conduct a largely manual surveillance, based on tools designed for other business monitoring activities. In order to comply with the new requirements, they had to acquire or develop IT-based monitoring systems that would enable them to screen the whole range of their business relationships, including transactions. The financial institutions that the assessors visited were still in the process of developing and adjusting the automatic monitoring systems. Notwithstanding the limits of existing tools, financial institutions mentioned examples of suspicious operations which had been detected and analyzed. All financial institutions maintain close relationships with the head of the A-FIU who is regularly contacted on problematic cases and provides guidance on how to deal with them, especially on whether they should be reported or not.

***Special Attention to Countries Not Sufficiently Applying FATF Recommendations (c. 21.1 & 21.1.1); Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose from Countries Not Sufficiently Applying FATF Recommendations (c. 21.2)***

591. There is no explicit requirement to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations, to examine the background and purpose of those transactions, and to make written findings available to competent authorities. The authorities consider that such operations would fall under the overall risk-based approach, leaving to financial institutions the decision to detect and analyze them, as well as to record their findings. They mention notably Article 40, paragraph 2b of the BWG and Article 98b, paragraph 4 of the VAG which require financial institutions to subject their business or transactions to risk analysis “using suitable criteria (in particular ... geography).”

592. The authorities also point to Article 40, paragraph 4, no. 2 of the BWG -and Articles 6 and 12, paragraph 4 of the WAG, referring to the BWG-, and Article 98b, paragraph 8, no.2 of the VAG which demand that credit institutions and domestic financial institutions report to the FMA countries which legislation does not permit customer identification as required under the BWG, and take

additional measures to handle the ML/FT risk effectively. The scope of this requirement is limited to identification issues and does not address all requirements of the Standard.

593. The MoF sent the WKO a list of countries which are under FATF scrutiny, or issued advisory callings, recommending increased attention in dealing with institutions located in those jurisdictions. Since November 28, 2008, the FMA posts on its website the FATF and Moneyval statements on countries which AML/CFT regimes are deficient. The authorities consider that, on the basis of their advisory notices, financial institutions should include obligations set out in c.21.1 in their risk-based approach, and would be subject to sanctions for not doing so.

594. When meeting with financial institutions, the assessors found evidence of attention given to operations with persons from or in countries which do not or insufficiently apply the FATF Recommendations. Most financial institutions referred to the lists of countries received from the WKO, and some internationally-active banks include country risk among their internal ML/FT risk criteria.

595. However, as for Recommendation 11, the nature and the extent of diligence are not defined in laws, regulations or other enforceable means. The authorities underscore that the requirements defined in c.21.2 are *de facto* met by financial institutions which, when requested, have to prove to the supervisors that special attention has been given to those transactions in their risk-based approach. In the assessors' view, such construction does not correspond to the requirements of the criteria which call for direct obligations.

***Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 21.3)***

596. Article 78, paragraph 8 of the BWG, requires the Federal Government, in cooperation with the Main Committee of the National Council, to issue a regulation designating as NCCTs jurisdictions which do not take AML/CFT measures requested by the international standards. A violation of international standards shall in particular be assumed if the Council of the European Union or the FATF has adopted resolutions to this effect. Pursuant to paragraph 9 of the same Article, various measures could be applied to persons who have their residence or are incorporated in a NCCT, notably a ban on management positions or qualifying participation in a credit institution, interdiction of non-face-to-face business relationships, reporting of all transactions equal to or above EUR 100,000, and prohibition of simplified CDD measures. The Federal Government issued regulations based on Article 78, paragraph 8 of the BWG in 2002 (Nauru) and 2003 (Myanmar).

**3.6.2 Recommendations and Comments**

597. The authorities should:

**Recommendation 11**

- Define in law, regulation or other enforceable means a requirement for financial institutions to examine the background and purpose of all complex, unusual large transactions, or patterns of transactions, that have no apparent or visible economic or lawful purpose, and to keep resulting findings for at least five years.

- For insurance undertakings, extend the requirement to monitor transactions to all unusual patterns of transactions.

### **Recommendation 21**

- Define in law, regulation or other enforceable means, a requirement for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations, to examine the background and the purpose of those transactions which have no apparent economic or visible lawful purpose and to keep written findings.

### **3.6.3 Compliance with Recommendations 11 & 21**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R.11</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• No explicit requirement in laws, regulations or other enforceable means to examine as far as possible the background and purpose of all complex, unusual large transactions, or patterns of transactions, that have no apparent or visible economic or lawful purpose, to set forth findings in writing and to keep such findings for at least five years.</li> <li>• Monitoring of unusual patterns of transactions not required for insurance undertakings.</li> <li>• Concerns about the effectiveness of the provisions which were introduced recently.</li> </ul>
<b>R.21</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• No specific requirement in law, regulation or other enforceable means to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations.</li> <li>• No explicit requirement in laws, regulations or other enforceable means to examine as far as possible the background and purpose of transactions with persons from those countries, which have no apparent economic or visible lawful purpose, to set forth and keep findings.</li> </ul>

### 3.7 Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 & SR.IV)

#### 3.7.1 Description and Analysis<sup>32</sup>

##### Legal Framework

598. Relevant provisions concerning suspicious transaction reports are contained in Article 41, paragraph 1, no. 1 of the BWG, Article 98f, paragraph 1, nos. 1 and 2 of the VAG, Articles 6 and 12, paragraph 4 of the WAG (which refers to Article 41 of the BWG)<sup>33</sup>, Article 25, paragraph 5 of the BörseG and 365 u(1)1 of the GewO, covering all Austrian financial institutions.

##### *Requirement to Make STRs on ML to FIU (c. 13.1)*

599. The requirement is a direct mandatory obligation that is broadly the same for every profession. All have to report their suspicions of ML to the Federal Ministry of Interior. As explained in section 2.5.1, the common practice is that STRs are reported to the Austrian Financial Investigation Unit (A- FIU). The obligation, which refers to Article 165 of the StGB, covers all predicate offenses that are required to be included by the standard, except for counterfeiting and piracy of products (see the analysis of R.1 in section 2 for more details). A common feature is that the reporting requirements always refer to a suspicion in relation to money laundering. There is no mention of the relation to the proceeds of a criminal activity. But some differences should also be noted among all laws.

600. In the BWG, the VAG and the BörseG, the reporting obligation refers to “Article 165 of the StGB – including asset components which stem directly from a criminal act on the part of the perpetrator.” According to the authorities, this provision is intended to oblige financial institutions to also report cases where there is a suspicion of self-laundering. The GewO only mentions Article 165 of the StGB.

601. In the BWG, the VAG and the BörseG, a financial institution is obliged to report when it “suspects or has reasonable grounds to suspect” that a transaction serves the purpose of ML. Insurance brokers covered by the GewO are obliged to report when “they know, suspect or have reasonable grounds to suspect.” In the BWG, the VAG and the BörseG, the obligation is related to a “transaction that serves the purpose of ML” when in the GewO it relates to a suspicion that ML “is being or has been committed.”

602. In addition to the relation to a transaction, the VAG also requires that a report has to be made in case of suspicion “that the intended establishment of a business relationship or an existing business relationship serves the purpose of money laundering (Article 165 StGB—including asset components

---

<sup>32</sup> The description of the system for reporting suspicious transactions in section 3.7 is integrally linked with the description of the FIU in section 2.5 and the two texts need not be duplicative. Ideally, the topic should be comprehensively described and analyzed in one of the two sections, and referenced or summarized in the other.

<sup>33</sup> As the WAG refers to the BWG concerning reporting requirements, each subsequent reference to the BWG includes the legal framework applying to investment firms and investment service providers.

which stems from a criminal offense committed by the perpetrator himself).” This covers the specificities of the insurance business.

603. While 1,045 STRs were filed by reporting entities from the financial sector in 2007, the number of STRs is relatively lower than that in comparable countries. It has to be noted that the statistics on the number of STRs include all information received by the financial and non-financial institutions. For example, information on phishing emails and “419 letters” accounted for around 200 STRs in 2007. In addition, credit institutions are the main provider of information, with only six STRs from insurance undertakings and none from the other reporting entities of the financial sector. Concerning the STRs from the credit and domestic financial institutions, the authorities were not able to provide information regarding the breakdown by type of activities, or regarding the number of banks that declared suspicions. Meetings with reporting entities lead to the view that the situation is very uneven. While banks that are considered of systemic importance by the authorities may only disclose one or two STR a year, the few credit institutions specialized in money transfer services reported 392 STRs in 2007. For 2008, one single reporting entity was on a 40 STR/month basis. Without the money transfer sector, that leaves the total for the rest of the credit and domestic financial institutions with less than 650 STRs in 2007 and less than 450 if phishing emails and “419” letters are deducted. It appears that the major factor triggering those STRs is the involvement of offshore business, with 218 of the reports received in 2007.

Statistical Table 24. Origin of STRs

	2004	2005	2006	2007
<b>Credit institutions</b>	349	417	651	1039
<b>Insurance undertakings</b>	11	9	7	6
<b>Others (securities institutions, insurance intermediaries)</b>	0	0	0	0
<b>Total</b>	360	426	658	1,045

604. Different reasons are given by the authorities to explain this low level of reporting, that they generally regard as satisfactory and producing high quality reports. For non-banking financial institutions, the need for more training is acknowledged and subject to the availability of resources. Concerning the banks, the low level of STRs is partly explained by the functioning of the system. It is very common that banks call the A-FIU in case of unusual transactions in order to receive more guidance on a specific case. Based on its expertise, the A-FIU will give a non-binding advice to the bank on the necessity to report or not. The A-FIU receives on average 10 calls every day. On the other hand, it happens that the A-FIU, with its law enforcement knowledge of the criminal activities, calls a bank to inform about a particular situation that may trigger an STR. This flexible approach between financial institutions and the A-FIU was encouraged by the FMA in its 2004 guidance on controls and STRs. Section 42 of the guidance recommends “that credit institutions maintain regular contact with the FIU in order to be able to benefit from the FIU’s expert knowledge in identifying and assessing risk profiles as well as unusual business arrangements.” The phone numbers of the A-FIU are provided in the guidance. Another reason for the low level of reporting is that it was no clear obligation to monitor business relationships and transactions in the previous versions of the laws. Consequently, financial institutions had initially no reason to implement IT tools and they started this

year buying or developing such monitoring systems, which could lead to the detection of more suspicious cases.

605. The assessors also understood that the criminal procedure rules in Austria could be a structural factor explaining the low level of STRs. Indeed, a report qualifying as STR, as defined in the relevant laws (the financial institution suspects or has reasonable grounds to suspect that a transaction serves the purpose of ML or FT), has to be considered by the police as a complaint. Accordingly, when informed of a possible dangerous attack (Article 16 SPG) or made aware of the suspicion that a person has committed an offense (Article 1(2) of the StPO), the police has to conduct an investigation (SPG) or a criminal investigation (StPO), which is subject to information of the Public prosecutor's office pursuant to Articles 99 and 100 of the StPO. This explains that a large number of public and private entities met by the assessors mentioned *Anzeige* (complaint) when referring to STRs. When the case is closed by the prosecutor or the preliminary proceedings end, the suspect/defendant is informed and authorized to view all the files related to the investigation (Article 194 of the StPO), including the STR. Article 100(3) mentions that the report by the police to the prosecutor has to mention "the names of the person who filed the criminal complaint, names of the victims and, if applicable, other informants", which includes the reporting entity. The structure of the criminal procedure, and the fact that the police is legally bound to investigate on every report on suspicion that a transaction serves the purpose of ML or FT, which means that ultimately the customer will be informed of the STR and of its origin, is a factor of self-limitation for reporting entities. Reporting entities met by the assessors acknowledge that this explained the need for an elaborated and objective suspicion in order to report. Consequently, one solution found by some reporting entities is to call the A-FIU for advice when they face an unclear situation and to file a STR if they have tangible elements supporting the suspicion. Even if this process seems flexible, it may contribute to discourage financial institutions from filing STRs, explaining their low level. Another explanation given to the assessors by reporting entities was related to cases of disclosure of the reporting entity's name to the suspected person by the local police investigating a STR.

606. In response to these weaknesses, the authorities agreed on November 6, 2008 on a joint action plan between the MoF, the A-FIU, the MoJ, the FMA, the BVT, the Federal Chancellery and the private sector. It contains measures to promote the protection of reporting entities and their employees: awareness raising campaigns among the law enforcement authorities, public prosecutors, judges and the private sector, ordinances by the MoJ and the Federal Chancellery, ways to promote "anonymity" of STRs, and information on protective mechanisms contained in the StPO. On the latter, an ordinance has been issued by the MoJ on November 11, 2008 and addressed to public prosecutors and judges. The right of the suspect/defendant to view all the files related to the investigation can be delimited or certain data can be made anonymous, when there is danger for the personal security of an involved participant or there are higher interests of data protection. (Article 51, paragraph 2 and Article 68, paragraph 1 of the StPO). But according to Article 51(2) of the StPO, a restriction of the right to access to files is inadmissible if the suspect is in detention.

607. In addition, in the absence of a structured study on the specific risks faced by financial institutions in Austria, it is difficult to tailor supervision and training in order to raise the awareness of the ones that may be more at risk. For example, and at the difference of other countries with a lot of tourists, neighboring countries using different currencies, intensity of the use of cash in the economy and importance of the cash couriers, the 12 credit institutions specialized in currency exchange did

apparently not provide STRs and have not been subject to specific information on exposure to ML risks and supervision in the recent years.

***STRs Related to Terrorism and its Financing (c. 13.2 and c. IV.1)***

608. The direct mandatory obligation to report STRs also applies to terrorism financing, pursuant to the Articles mentioned regarding c.13.1. There are four different texts that apply to the various types of financial institutions. Under the BWG and the VAG, the reporting obligation is applicable when there is a suspicion or reasonable grounds to suspect “that a customer belongs to a terrorist group pursuant to Article 278b StGB or that a transaction serves the purpose of terrorism financing pursuant to Article 278d StGB.” However, due the fact that the reporting obligation includes a cross-reference to the definition of TF in the criminal code, the technical shortcomings noted in paragraphs 184–186, *infra*, could conceivably influence a financial institution’s decision on whether to file a report. As a practical matter, the assessors are convinced by the authorities’ explanation that the broad definition, quoted above, will override this largely theoretical concern. Nevertheless, as noted in the discussion of SR II, the authorities should consider enacting technical amendments to section 278d of the criminal code. They should also consider providing further guidance to foreclose the possibility that the reporting provisions could be misinterpreted.

609. The BörseG only mentions a reporting obligation regarding the suspicion or the reasonable grounds to suspect that a transaction serves the purpose of FT. This text is more limited than the text in the reporting obligations applicable to credit institutions and insurance undertakings since it does not explicitly extend to situations where customers are suspected of belonging to a terrorist organization. Nevertheless, the broad reference to “serving the purpose of FT” suffices, as a practical matter, to cover this situation.

610. The reporting obligation in the GewO refers to the suspicion or the reasonable grounds to suspect that “terrorism financing is being or has being committed.” In the latter case, terrorism financing is defined in Article 365n, paragraph 2 as “the provision of a financial contribution to support a terrorist group pursuant to Article 278b StGB, to commit a terrorist offense pursuant to Article 278c StGB or to complete the offense pursuant to Article 278d StGB.”

611. STRs concerning the financing of terrorism have been a relatively small percentage of the total, amounting to 23 in 2007. Only parts of these reports are related to the name lists with a number of false positive considered to have decreased due to the increased precision of the lists. The reporting entities mentioned to the assessors that they both report on the ground of FT when there are possible relations with the lists, but also on other grounds such as a possible relation with a terrorist organization, a zone of conflict or a sensitive NPO.

Statistical Table 25. STRs investigated by the BVT

	<b>2004</b>	<b>2005</b>	<b>2006</b>	<b>2007</b>
Credit institutions	9	16	14	20
Money transmitters	3	3	1	3
<b>Total</b>	<b>12</b>	<b>19</b>	<b>15</b>	<b>23</b>

***No Reporting Threshold for STRs (c. 13.3, c. IV.2)***

612. Reporting obligations mentioned in c.13.1 and c.13.2 apply irrespective of any threshold. The requirement to report all suspicious transactions, including attempted transactions, is addressed using different terms for each of the financial institutions. Article 365u, paragraph 1 of the GewO mentions “*zu begehen versucht*” while Article 41, paragraph 1 of the BWG, Article 98f paragraph 1 of the VAG and Article 25, paragraph 5 of the BörseG mention “*bevorstehende*.” The authorities confirmed that both expressions are relevant to cover attempted transactions.

613. Financial institutions that the assessors met insisted on the strict selection criteria they apply when entering into a business relationship, and their common practice to decline a business when doubts persist on the information received. None of them considered filing an STR on these potential customers. However, for the authorities they were legally required to do so and the A-FIU indicates it receives reports on attempted transactions and declined businesses, but the number is very low.

***Making of ML and FT STRs Regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2)***

614. Austria did not adopt an all crimes approach for underlying offenses and Article 165 only refers to specific offenses. These include two tax offenses related to international trade, smuggling and the evasion of import or export taxes. This applies insofar as these offenses fall within the competence of the courts, that is when the value of the evaded duties exceeds EUR 37,500. Evasion of income tax, corporate tax, VAT or excises duties, is not a predicate offense for ML, even when tax evasion amounts to a crime in Austria, which is when the value of the evaded taxes exceeds EUR 500,000. This said, the laws do not provide for any exception of STR reporting requirement by reason of tax related matters.

***Additional Element—Reporting of All Criminal Acts (c. 13.5)***

615. The reporting requirements mentioned in the BWG, VAG, BörseG and GewO include transactions that are suspected to serve the purpose of money laundering as defined under Article 165 of the StGB. Consequently, the requirement to report includes the laundering of the proceeds of all criminal acts that would constitute a predicate offense for money laundering in Austria. But the reporting obligation does not require financial institutions to report funds that are the proceeds of the criminal acts that are listed in Article 165 if there is no element demonstrating that the transaction serves the purpose of money laundering.

***Protection for Making STRs (c. 14.1)***

616. According to Article 41, paragraph 7 of the BWG and Article 98f, paragraph 8 of the VAG, claims for damages shall not be permitted based on the circumstance that a bank, insurance, investment or securities company, or its employees, delayed or failed to execute a transaction on the negligent lack of knowledge that the suspicion of money laundering or terrorism financing was wrong. The notion of employees covers every staff in contractual relation with a company, including the management. Credit institutions and other financial institutions are legal persons and can as such act only through their directors, officers and employees. The provisions of Article 25, paragraph 10 of the BörseG are identical, except that it only protects concerning suspicion of money laundering.

617. In addition banks and their employees are protected from a breach of the banking secrecy when reporting their suspicions, as Article 38, paragraph 2, no. 2 BWG states that the obligation to maintain the banking secrecy does not apply in the case of obligations to provide information pursuant to Article 41, paragraph 1. Consequently, they are protected from both criminal and civil liability for making STRs. There are no comparable secrecy requirements regarding investment, securities and insurance companies.

618. According to Article 365u of the GewO, the reporting of suspicions by insurance intermediaries shall not constitute any breach of any restriction on disclosure of information imposed by contract, or by any legislative, regulatory or administrative provision, and shall not lead to a liability of any kind. There is no mention on the necessity to have reported in good faith to the A-FIU.

***Prohibition against Tipping-Off (c. 14.2)***

619. In order to prevent potential perpetrators from being warned, Article 41, paragraph 3b of the BWG, Article 98f, paragraph of the 5 VAG, and Article 25, paragraph 8 of the BörseG, financial institutions and, by extension, their employees, are prohibited from disclosing to their clients or third parties the fact that an STR or any related information such as requests for additional information have been reported or provided to the A-FIU or the police. This prohibition extends to third parties. In cases where an order to suspend or cancel the transaction is issued by the police according to Article 41, paragraph 3b of the BWG, Article 98f, paragraph 3 of the VAG, and Article 25, paragraph 7 of the BörseG, financial institutions may refer the customer to the police. They are nevertheless prohibited to disclose the fact that an STR has been filed.

620. The prohibition does not apply to disclosures:

- towards the FMA, the OeNB, and for law enforcement purposes;
- between financial institutions belonging to the same group as defined in Article 2 (12) of Directive 2002/87/EC and bound by obligations of the Third EU ML Directive or obligations equivalent to those set forth in the Third EU ML Directive and supervised for compliance with these obligations;
- in cases related to the same customer and the same transaction involving two or more institutions, between the relevant institutions provided that they are bound by obligations of the Third EU ML Directive or obligations equivalent to those set forth in the Third EU ML Directive and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged is to be used exclusively for the purposes of the prevention of ML and FT.

621. The last two exemptions meet concerns that ML and FT are international phenomena and efficient AML/CFT systems should therefore bear in mind that criminals might access national (financial) markets via branches and subsidiaries of financial institutions operating in various countries. Therefore, Articles 31, paragraphs 1 and 34, paragraph 2 of the Third EU ML Directive require financial institutions to apply AML/CFT measures at least equivalent to those set out in the Directive, and to communicate relevant policies and procedures to their branches and subsidiaries abroad (implemented in Article 40, paragraph 4, no. 1 and Article 41, paragraph 4, no. 2 of the BWG, Article 98b, paragraph 8, no. 1, and Article 98h, paragraph 1, no. 2 of the VAG and Articles 6 and 12,

paragraph 4 of the WAG). In addition, it appears from the meetings with reporting entities that in a country like Austria with a strong banking secrecy but a large number of financial institutions belonging to the same group, these provisions enable those financial institutions to exchange information on STRs and other related information, with the view to enhance the detection of suspicious transactions.

622. On November 4, 2008, the FMA published a list of countries applying equivalent AML/CFT standards in order to implement Article 40, paragraph 8 and Article 40a, paragraph 8 of the BWG. But no guidance has been given to financial institutions regarding the implementation of Article 41, paragraph 3b of the BWG, Article 98f, paragraph 3 of the VAG, and Article 25, paragraph 7 of the BörseG. The cases described in those Articles are broader than what is described in Article 40, paragraph 8 of the BWG, because Austrian financial institutions have to determine if another financial institution is bound by the obligations of the Third EU ML Directive or obligations equivalent to those set forth in the Third EU ML Directive, supervised for compliance with these obligations, and subject to equivalent obligations as regards professional secrecy and personal data protection. The FMA explained to the assessors that Austrian credit institutions are not allowed to determine themselves if another financial institution is bound by the obligation equivalent to those set forth in the Third EU ML Directive. They are restricted to the countries of the list. This has been clarified by FMA in the circulars addressed to credit institutions and insurance companies “*Rundschreiben zur Feststellung und Überprüfung der Identität für Kreditinstitute*“ and “*Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen*“ (Recital 55 in both guidance).

623. Article 365x, paragraph 1 of the GewO determines that the insurance intermediaries, and where applicable, their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Article 365u of the GewO or that a ML or FT investigation is being or may be carried out. Pursuant to Article 365x, paragraph 2 of the GewO, this prohibition does not include the competent authorities or disclosure for law enforcement purposes.

***Additional Element—Confidentiality of Reporting Staff (c. 14.3)***

624. According to Article 20, paragraph 3 of the B-VG, authorities are obliged to secrecy about all facts of which they have obtained knowledge exclusively from their official activity, save as otherwise provided by law. Any breach of this secrecy provision entails disciplinary (sanctions up to dismissal) and criminal proceedings (Article 310 of the StGB “disclosure of official secrets”, sanctioned by up to 3 years of imprisonment). According to the provisions of the StPO, the STR has to be forwarded with the case when the investigation is opened and stays in it. On the basis of Article 52, paragraph 2 of the StPO (witness protection), it is possible to restrict access to records by the suspect during the investigation. The right to access to files may be limited only until conclusion of the preliminary proceedings and only in so far, as special circumstances allow the reasonable assumption that the purpose of the inquiries would be endangered by an immediate inspection of certain documents. When the case is closed by the prosecutor or the preliminary proceedings end, the suspect/defendant is informed and authorized to access all files related to the investigation, including the STR. In practice, financial institutions are encouraged to mention the name of the compliance or head of the legal department instead of the name of other employees when reporting an STR to the A-FIU. This practice has been encouraged by the November 11, 2008 MoJ Ordinance (section 4.2).

***Consideration of Reporting of Currency Transactions above a Threshold (c. 19.1 to 19.3)***

625. In November 2007, representatives of all Austrian authorities concerned with money laundering prevention (MoF, MoI, MoJ, MoE, FMA and OeNB) analyzed the advantages and disadvantages of implementing an automated reporting system, including for currency transactions.

626. As a result of this analysis, competent authorities concluded that the introduction of an automated reporting system—either on the basis of threshold values or on other criteria—as set out in FATF Recommendation 19 is currently not recommended. A document titled “Minutes of the Meeting on FATF Recommendation 19 (OeNB, November 30, 2007)” was subsequently distributed. The conclusions were supported by the following elements:

- The authorities considered that reporting systems currently in place in Austria are comparable to automated reporting systems, such as mandatory reporting of certain legal transactions (e.g., re. real estate and company law) to public registers, automated reporting requirements regarding withdrawals from savings accounts under certain conditions (Article 41, paragraph 1a BWG) and not previously disclosed fiduciary transactions (Article 41, paragraph 1, no. 2 BWG, Article 98f, paragraph 1, no. 3 VAG, Articles 6 and 12, paragraph 4 WAG, Article 8b RAO and Article 36b NO);
- The representative of the MoI emphasized the high quality of the Austrian system of reporting suspicious transactions and considered doubtful whether an automatically generated reporting system would in fact provide enough additional useful information. On the contrary, the view was that such system could affect the presently high quality of STRs in a negative way;
- Finally, the authorities considered that when implementing a mass reporting system, the data reported has to be analyzed with due care requiring substantial additional human and financial resources which might not be reasonable in relation to the added value.

627. Nevertheless, the authorities decided that the utility and feasibility of implementing an automated reporting system will be subject to further evaluation.

***Guidelines for Financial Institutions with respect to STR and other reporting (c. 25.1)***

628. The A-FIU is the main provider of information to financial institutions, either through its comprehensive annual report or through direct training sessions. The annual reports contain a description of the most common ML techniques and methods, as well as new trends or subject of interest identified by the A-FIU. To this regard, the 2007 annual report mentions Islamic banking and new payment technologies. It should be noted that when mentioning “419 letters” and phishing emails as part of the ML typologies in its annual report, the A-FIU may confuse reporting entities on the requirements of an STR according to Article 41(1) of the BWG and others. Additional information is given through training sessions. Around 20 such sessions are organized every year. Some are directed to all reporting entities, and some specific to the need of particular entities. During the last three years, specific training sessions have been offered to representatives of money transfer services, companies, banks, leasing companies and insurance companies. On top of this, compliance officers of reporting entities contact the officer on duty of the A-FIU on a regular basis (10 calls per day) in order to discuss new and current occurrences.

629. The FMA also addresses the questions from the reporting entities during its company visits. In 2004, the FMA issued circulars on Controls and Suspicious Transaction Reports (credit institutions and insurances). Circulars from the FMA are sent to the MoE that forwards them to the chamber of commerce competent for insurance intermediaries. It contains guidance for credit institutions on reporting requirements where there is ground to suspect violation of the AML/CFT requirements. But it has not been reviewed after the changes in the law. In particular, the introduction of a subjective suspicion test may require further guidance.

***Feedback to Financial Institutions with respect to STR and other reporting (c. 25.2)***

630. General feedback is available in the annual reports of the A-FIU that contain statistics on the number of disclosures and on the results of the disclosures, information on current techniques, methods and trends and sanitized examples of actual money laundering cases.

631. In addition, the A-FIU provides specific feedback. On the occasion of implementing the Third EU ML Directive new provisions were inserted to oblige the A-FIU to provide, wherever practicable, timely feedback on the effectiveness of and follow-up to STRs on ML and FT (Article 41, paragraph 4 of the BWG, and Article 98h, paragraph 2 of the VAG). The authorities expect that these provisions will further enhance feedback mechanism and institutionalize the current tools and instruments. For the time being, upon the receipt of an STR the A-FIU regularly contacts the reporting entity often requesting further documents (signature sample sheet, ID-documents, customer contact data, behavior of client when opening the account, account movement summary, cash withdrawals, vouchers, etc.) required for investigations. This opportunity is also used for giving immediate feedback, and helps the reporting entities to enhance the quality of the reporting.

**3.7.2 Recommendations and Comments**

632. The authorities should:

**Recommendation 13**

- Extend financial institutions' requirement to report to the A-FIU in order to cover all situations when there is a suspicion that funds are the proceeds of a criminal activity, and not only when there is a suspicion that a transaction serves the purpose of money laundering;
- Apply the obligation to make a STR to funds that are the proceeds of piracy and counterfeiting, and require professions under the GewO to report STRs in case of self-laundering;
- Supervisors should issue guidance to clarify that the reporting obligations extend to situations where persons are suspected of being a terrorist or belonging to a terrorist organization;
- As noted in the discussion of SR II, authorities should clarify and strengthen criminal law requirements concerning liability for financing individual terrorists and terrorist organizations; and
- Increase effectiveness of the reporting system and mitigate the current self-limitation of reporting entities due to the criminal procedure rules.

**Recommendation 14**

- Apply the protection for STR reporting only in case of good faith for insurance intermediaries;
- Prohibit a financial institution to refer a customer to the police when a transaction has been suspended following an STR.

**Recommendation 25**

- Update FMA guidance on reporting

**Special Recommendation IV**

- Supervisors should issue guidance to clarify that the reporting obligations extend to situations where persons are suspected of being a terrorist or belonging to a terrorist organization.
- As noted in the discussion of SR II, authorities should clarify and strengthen criminal law requirements concerning liability for financing individual terrorists and terrorist organizations.

**3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R.13</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Reporting requirement not on funds that are the proceeds of a criminal activity, but limited to transactions that serve the purpose of ML</li> <li>• No requirement to make an STR regarding funds that are the proceeds of piracy or counterfeiting. The GewO does not require to report STRs in case of self-laundering.</li> <li>• Provisions in three of the four different reporting laws raise technical issues that could affect institutions' decisions on whether they are obliged to file reports in relation to FT in certain situations.</li> <li>• Effectiveness questions raised by the low level of STRs.</li> </ul>
<b>R.14</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• The protection for STR reporting applies in the absence of good faith for insurance intermediaries.</li> <li>• The possibility to refer the customer to the police when a transaction is suspended creates an indirect "tipping off."</li> </ul>
<b>R.19</b>	<b>C</b>	
<b>R.25</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• No up-to- date guidance on reporting for credit and domestic financial institutions, insurance undertakings, and securities institutions.</li> </ul>

SR.IV	LC	<ul style="list-style-type: none"> <li>Provisions in three of the four different reporting laws raise technical issues that could affect institutions' decisions on whether they are obliged to file reports in certain situations.</li> </ul>
-------	----	--

### **Internal controls and other measures**

## **3.8 Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22)**

### **3.8.1 Description and Analysis**

#### **Legal Framework**

633. The Austrian supervisory framework contains a range of provisions requiring financial institutions to establish adequate internal policies, procedures and controls, compliance arrangements and recruitment policies together with ongoing employee training and internal audit functions to prevent and forestall money laundering and the financing of terrorism. The BWG acts as the lead law covering not only banking business but the wider Austrian definition of credit institution, with the anti money laundering provisions of the BWG often being referred to in other sector supervisory laws and adopted as the relevant standard. Additional provisions appear in the VAG and WAG in respect of insurance and securities business.

634. The internal controls and compliance arrangements likely to reduce the risks of money laundering and terrorist financing first appear in Articles 39(1), and 39(2)(b)(5) of the BWG, where credit institutions are required to introduce systems and controls to manage operational risk. Operational risk can reasonably be taken to include ML/FT risks, but the overarching reputation risk embedded into AML/CFT preventive measures is not addressed. Additionally, Article 41(4) 1-6 of the BWG specifically requires credit and domestic financial institutions to establish and maintain systems and controls to prevent money laundering and terrorist financing. Article 98(h) 1 of the VAG addresses similar matters in respect of insurance companies, while Article 6 of the WAG is the relevant Article in respect of securities institutions.

#### ***Establish and Maintain Internal Controls to Prevent ML and FT (c. 15.1, 15.1.1 & 15.1.2); Independence of Compliance Officer (c. 15.5)***

#### **Credit and Domestic Financial Institutions**

635. Articles 39 and 41, paragraph 4, nos. 1–6 of the BWG require credit institutions and domestic financial institutions to establish adequate risk management systems and appropriate policies and procedures to “forestall and prevent operations relating to money laundering or terrorist financing.” Article 41 includes the obligation to communicate these, in general terms, within the organization, and Article 41, paragraph 4, no. 2 specifically requires them communicated to branches and subsidiaries.

636. The BWG requires at Article 41, paragraph 4, no. 6 that a “special officer” is nominated within the institution to ensure compliance with the Article 40, et seq. measures for the suppression of money laundering and terrorist financing. The law is silent as to the seniority of the person appointed,

to its right to access all relevant information, and to the arrangements regarding his independence and direct reporting line to the senior management or the board of directors of the institution.

637. An explanatory note to Article 41, paragraph 4 of the BWG (Comments-Special Part 32 of the Annexure, Legislative Period XXIII) states that the AML compliance officer has to report back directly to the board of directors. The authorities indicated that, as a general legal principle in Austria, all explanatory notes to the law form by-part of the legal texts and are used for their interpretation. However, this explanatory note adds a new requirement to the legal provisions, and, while in the FMA's view, this obligation would be enforceable, there has been no case where a sanction was taken by the FMA on this sole basis.

638. These matters are also addressed in FMA Circular on control Procedures and STRs in connection with ML/FT, dated April 23, 2004, which envisage an AML Compliance Officer who is properly competent, sufficiently independent as to be able to execute his/her function, is authorized to represent the institution on AML matters to the authorities, and is authorized to issue instructions within the institution on AML matters, and to have direct access to senior management. The Circular provides also in Article 15 that the AML officer should be authorized to conduct inspections and be able to "obtain, request and examine information." Additionally, he/she should have the power to stop transactions, if necessary. While relevant statements, the FMA would, however, have to rely on the general risk management requirements in Article 39, paragraphs 1 and 2 and Article 41 to enforce these matters, as the current guidance is not directly enforceable (see above section 3.1.1), and the provisions of the Circular related to the "anti-money laundering official" build upon the content of the Extended Due Diligence Declaration issued in 1992 by the Austrian Banking industry; at that time, the BWG did not contain any provisions related to the compliance officer.

639. The FMA intends to release guidance indicating that it believes the AML Compliance Officer needs internal inspection powers in order for the organization to meet the FMA's interpretation of the overall requirement under Article 40, of the BWG to have satisfactory risk management systems with regard to the prevention of money laundering and terrorist financing.

### **Securities Institutions**

640. As outlined above, Article 6 of the WAG imports Articles 39 and 41 from the BWG and applies them to investment firms and investment services undertakings. Article 39 places a general obligation on the managers of a credit institution, and therefore by its adoption in WAG, on the managers of investment firms and investment services undertakings to have a general, overarching risk management framework. It is oriented heavily to the needs of a credit institution and may not translate effectively to the needs of an investment business. For example, Article 39, paragraphs 2b and 2c, and 4 sets out specific risks a credit institution must take into account but these are difficult to apply to an investment services business, yet other relevant general risks that would be relevant to securities businesses are not mentioned.<sup>34</sup> Article 41, paragraph 4, nos. 1–6 of the BWG set internal

---

<sup>34</sup> The FMA is in the process of proposing amendment of the general reference to the AML/CFT provisions of the BWG (Articles 6 and 12 paragraph 4 of the WAG).

control requirements for AML/CFT measures which are applicable to securities institutions with the same caveat as mentioned above for credit institutions and domestic financial institutions.

641. Additionally, the WAG defines general organizational norms for all securities institutions: Article 17 of WAG sets the requirement to establish a general organization framework for the institution, Article 18 focuses on compliance arrangements and Article 19 turns particularly to risk management. In accordance with Article 18, paragraph 4, no. 1, the person assigned to the general compliance function must have the necessary authority, resources and expertise, and have access to all relevant information. For matters relating to the AML/CFT compliance officer, it is necessary to go to imported Article 41, paragraph 4 of the BWG commented above.

### **Insurance Undertakings**

642. The VAG Article 98(h) requires that an insurance institution establishes a general framework of policies and procedures relating to customer due diligence, reporting, record keeping, internal control, risk assessment, risk management and compliance management. The Article requires these policies are communicated branches and subsidiaries and disseminated to staff. The Article provides also for the appointment of an Anti-Money Laundering Compliance Officer.

643. The legal provisions which apply to financial institutions do not define the compliance officer function as a management position, able to act independently and reporting to senior management or to the board of directors. The officer's right to access CDD data and information, transaction records and other relevant information is not stated in any of the financial laws.

644. When meeting with financial institutions, the assessors were shown detailed AML/CFT procedures manuals, which have been developed in the recent years. All compliance officers who attended the meetings hold management positions and were in charge of conducting AML/CFT related investigations for which they had access to all relevant internal information. In some institutions, the compliance officer reports to the chairman of the management board on a semi-annual or annual basis.

### ***Independent Audit of Internal Controls to Prevent ML and FT (c. 15.2)***

#### **Credit Institutions**

645. Under the General Due Diligence Obligations, credit institutions are required to have appropriate administrative accounting and control procedures, the adequacy of which must be reviewed by the internal audit at least once a year (Article 39, paragraph 2). Article 42 (1) to (7) of the BWG sets out the expectations of credit institutions regarding internal audit functions. The primary provisions of the Article are that credit institutions set up an internal audit unit which reports directly to the directors and which serves the exclusive purpose of conducting ongoing and comprehensive reviews of the legal compliance, appropriateness and suitability of the institution; that the unit must be adequately resourced sufficient to fulfill its function (including provisions relating to the competency of internal audit staff); and that the unit must report directly to the supervisory board on a quarterly basis to report relevant matters including the results of the its audit work. The minimum mandatory areas for the audit review which are set out in the law at Article 42, paragraph 4, no. 3 include AML/CFT measures. There is no requirement for the audit to include sample testing

when testing compliance with AML/CFT. The above-mentioned provisions do not apply to domestic financial institutions.

### **Securities Institutions**

646. Article 20 of the WAG sets the requirement to establish an internal audit function that is separate and independent. The unit should create an audit plan to examine and evaluate the adequacy and effectiveness of the legal entity's systems and controls, issue recommendations and verify whether or not those recommendations have been implemented. The unit is required to report at least once per year to senior management outlining its activities and stating in particular if adequate measures have been taken to put right defects previously identified. No mention is made of auditing requirements specific to AML/CFT procedures and systems.

### **Insurance Undertakings**

647. Article 17(b) of the VAG requires that insurance institutes set up an internal auditing unit, which shall report on a quarterly basis directly to the management, and whose sole purpose shall be to continuously verify that the business is "lawfully, properly and expediently" conducted. It requires also that the insurance undertaking identifies, estimates and controls the "risks connected with the insurance activity." The provision introduces the requirement (not apparent in other laws) that orders concerning the internal auditing unit shall have to be jointly made by at least two management board members. Although Article 17(b) can be interpreted as broadly based, there is no mention specifically of ML/FT or other operational risks.

648. The authorities underline that AML/CFT provisions are included in the WAG, that securities firms are required to have in place policies and procedures to ensure compliance with the WAG, and that the adequacy and effectiveness of those policies and procedures are examined and evaluated by their internal audit. Still, the internal audit mandate is defined in general terms. Integrating AML/CFT compliance into the internal audit program is not specifically required from securities institutions and insurance undertakings, and modalities of examinations, such as sample testing, are not included into the requirements.

649. All financial institutions the assessors visited empower their internal audit departments to conduct frequent and regular reviews of the AML/CFT systems. In the audit process, auditors analyze procedures and internal controls, and check some files and documents, selected with IT-based analytical tools.

### ***Employee Training and Screening Procedures (c. 15.3 and 15.4)***

650. Both the BWG (Article 41(4)(3)) and the VAG (Article 98h (1)) make it an obligation for financial institutions to take appropriate measures to ensure staff awareness of AML/CFT provisions, and to train relevant employees to recognize and deal with transactions which may be connected to money laundering or terrorist financing. Articles 6 and 12, paragraph 4 of the WAG carry over the provisions of the BWG. Financial institutions that the assessors interviewed have such training programs in place for new employees, as well as on an annual basis for experienced staff. In most cases, ongoing training is provided through IT and includes some form of testing.

651. The laws do not specifically refer to the level of employee screening expected of an institution but do make reference to the importance of an institution making proper assessment of the capabilities of their staff. Industry members interviewed spoke of practical difficulties in carrying out screening of future and current employees. The authorities indicate that it is common practice for employers to ask for an extract from police records which can be obtained easily at each police office.

***Application of AML/CFT Measures to Foreign Branches & Subsidiaries (c. 22.1, 22.1.1 & 22.1.2); Requirement to Inform Home Country Supervisor if Foreign Branches & Subsidiaries are Unable Implement AML/CFT Measures (c. 22.2)***

652. All regulatory laws make clear that financial institutions must ensure that the measures applied at their branches and subsidiaries in third countries (non EU Member States) are at least equivalent to those set forth in the Austrian regulatory framework. Article 41, paragraph 4, nos. 1-6 of the BWG, and Article 98h, paragraph 1, no. 2 of the VAG require credit institutions, domestic financial institutions and insurance undertakings to establish adequate and appropriate policies and procedures to “forestall and prevent operations relating to money laundering or terrorist financing.” Article 41, paragraph 4, no. 2 of the BWG and Article 98h, paragraph 1, no. 2 include the obligation to communicate them to branches and subsidiaries in third countries. If a branch or subsidiary is unable to implement equivalent measures, they must inform the FMA, and take additional measures to handle the risk effectively. These provisions are contained within Article 40, paragraph 4, nos. 1 and 2 of the BWG, Article 98b, paragraph 8, nos. 1 and 2 of the VAG and Article 6 of the WAG. Since November 28, 2008, the FMA posts on its website the FATF and Moneyval statements on countries which AML/CFT regimes are deficient.

653. Discussions with industry on this point indicated certain countries to have lower standards than those in Austria and that the banks have informed the FMA that they are unable to implement group standards in the overseas operations. The authorities indicated that the FMA would not approve a participation in a foreign credit institution if the Austrian AML/CFT requirements could not be met. This has never been the case. Instead, an administrative ruling issued by the FMA may allow financial institutions to delay compliance with certain specific Austrian standards during “an appropriate period of time.” The delay, which aims at giving financial institutions enough time to implement the home country standard, lasts from a few weeks up to several months, depending on the circumstances. The authorities reported that there were only few cases where delays for implementing AML/CFT standards were extended further.

***Additional Element - Consistency of CDD Measures at Group Level (c. 22.3)***

654. There is no requirement for financial institutions to apply consolidated CDD measures at a group level. However, the first step in addressing this issue is to require that CDD and record keeping measures applied by their branches and subsidiaries located in third countries are equivalent to those applicable in Austria, which is done at Article 40, paragraph 4, no. 1 of the BWG, and Article 98b, paragraph 8, no. 1 of the VAG. Confidentiality which applies to STRs does not prohibit information exchange within a financial group or between financial institutions from a member state or a third country, provided that they belong to the same category and are subject to equivalent secrecy and data protection provisions (Article 41, paragraph 3b, nos. 2 and 3 of the BWG, and Article 98f, paragraph 5, nos. 2 and 3 of the VAG).

655. Evidence was found that financial institutions subject to core principles do not apply consistent CDD measures at group level due to certain countries' local laws precluding the application of equivalent AML/CFT procedures being applied in their foreign branches and subsidiaries. Additionally, cooperative groups, constituted of many different and independent credit institutions, clearly share a reputation risk, but are not able to consolidate customer information across their different legal entities.

### 3.8.2 Recommendations and Comments

656. Financial institutions should be required by law, regulation or other enforceable means to:

#### Recommendation 15

- Give the AML/CFT compliance officer the right to access CDD data and information, transaction records and other relevant information;
- Establish the compliance officer function as a management position;
- Integrate AML/CFT compliance into internal audit work, notably for securities and insurance businesses;
- Require domestic financial institutions to maintain an internal audit function; and
- Conduct adequate staff screening.

#### Recommendation 22

- Extend in laws, regulations or other enforceable means the obligation to apply provisions consistent with home country requirements and the FATF Recommendations to all AML/CFT requirements.

### 3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	PC	<ul style="list-style-type: none"> <li>• No ad-hoc provision in law, regulation or other enforceable means giving the compliance officer right to access CDD data and information, transaction records and other relevant information;</li> <li>• Lack of specific provisions establishing that the compliance officer is a management position;</li> <li>• No requirement for domestic financial institutions to maintain an internal audit function;</li> <li>• Insufficient integration of AML/CFT compliance into internal audit work for securities and insurance business; and</li> <li>• Inadequate staff screening requirements and practices.</li> </ul>

<b>R.22</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Obligation to apply equivalent AML/CFT provisions limited to CDD and record keeping measures.</li> </ul>
-------------	-----------	---

### 3.9 Shell Banks (R.18)

#### 3.9.1 Description and Analysis

*Prohibition of Establishment Shell Banks (c. 18.1); Prohibition of Correspondent Banking with Shell Banks (c. 18.2); Requirement to Satisfy Respondent Financial Institutions Prohibit of Use of Accounts by Shell Banks (c. 18.3)*

657. The BWG defines a shell bank as a credit institution incorporated in a jurisdiction in which it has no physical presence, that is, meaningful mind and management (Article 2 (74)). Articles 4 and 5 of the BWG set out the licensing criteria for banks in general. Article 5 requires banks to have their place of establishment and head office located in Austria (paragraph 1, no. 14), and to have one director who is resident in Austria (paragraph 1, no. 10). Additionally, the FMA may revoke the banking license if the business operations do not commence within twelve months or have not been conducted for six consecutive months (Article 6, paragraph 1 of the BWG). While the legal framework does not explicitly prohibit the establishment of shell banks, the requirements for issuing and maintaining a license for operating a banking business seem sufficient to preclude the establishment or the continued operation of a shell bank.

658. Article 40(d) prohibits credit institutions to enter into or continue a correspondent banking relationship with a shell bank and 40(d)(1) refers to a banking institution taking appropriate measures to ensure its banking correspondents, in turn, to not enter into arrangements with shell banks.

659. The assessors were not aware of any shell bank operating in Austria. Responses from industry indicated a cautious approach when opening correspondent banking relations.

#### 3.9.2 Recommendations and Comments

660. The recommendation is fully observed.

#### 3.9.3 Compliance with Recommendation 18

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R.18</b>	<b>C</b>	

### 3.10 The Supervisory and Oversight System—Competent Authorities and SROs. Role, Functions, Duties, and Powers (Including Sanctions) (R.23, 29, 17 & 25)

#### 3.10.1 Description and Analysis

##### Legal Framework

661. The legal framework for the supervision and regulation of reporting entities of the financial sector is set out in the Financial Market Authority Act (*Finanzmarktaufsichtsbehördengesetz, FMABG*) and in the sector-specific laws, that is, the BWG for the credit and domestic financial institutions, VAG for the insurance undertakings and the WAG for investment companies and investment services companies.

662. The FMA was established in April 2002 as the single regulatory body in charge of banking, insurance, securities and pension company supervision (Article 1 of the FMABG). It regulates and supervises all persons and entities that conduct the financial activities listed under the FATF definition of financial institutions, with the exception of insurance intermediaries which are regulated by the Trade Act (*GewO*) and domestic financial institutions which are regulated by the AVG. Both insurance intermediaries and domestic financial institutions are supervised by local district authorities.

663. The FMA was established as an autonomous institution under public law with its own legal personality, and is not bound by any instructions in the performance of its duties. Pursuant to Article 3, paragraph 2 of the FMABG, the FMA takes any and all supervisory measures that are necessary, expedient and appropriate after a due consideration of the specific circumstances. To this end, it must take care to maintain financial market stability. In the performance of its duties, the FMA may use the audit reports of the statutory auditors and bodies of the companies subject to its supervision, as well as the examination reports of the Austrian National Bank (*OeNB*).

664. The bodies of the FMA are: the Executive Board which consists of two members appointed by the Federal President and which is notably responsible for managing the entire operation of the FMA, as well as for representing the FMA in and out of courts (Article 4 to 7 of the FMABG); and the Supervisory Board, which consists of the chairperson, the deputy to the chairperson, four additional members and two co-opted members, and which, among other functions, supervises the organization and management of the FMA (Article 4, 8 to 12 of the FMABG).

665. Pursuant to Article 44b, paragraph 1 of the Federal Act on the Austrian National Bank (*Nationalbankgesetz, NBG*), the OeNB must, in the public interest, monitor all circumstances that may have an impact on safeguarding financial stability in Austria. In practice, supervision of financial institutions is the responsibility of the FMA, although offsite surveillance and onsite inspections of banks are carried out by the OeNB acting on its behalf.

666. The split in duties between the FMA and OeNB is best described as the split between authorization and enforcement matters on the one hand (FMA), and offsite analysis and onsite examinations on the other (OeNB). The FMA has responsibility for approvals and authorizations, although it is understood that the OeNB is, in practice, consulted on these decisions. Enforcement is carried out by the FMA. Within the FMA, Department IV2, International Affairs and European Integration, sits a Money Laundering Competence Center which monitors and contributes to national and international developments, delivers training, drafts guidance notes, and lends support to supervisory departments.

***Regulation and Supervision of Financial Institutions (c. 23.1) Designation of Competent Authority (c. 23.2)***

667. Credit institutions in Austria and those that are authorized in other EU Member States and which carry out activities in Austria are subject to regulation and supervision by the FMA pursuant to Article 1 and Article 2 of the FMABG and 69 of the BWG. Banking supervision involves “performing the official tasks and exercising the powers which are assigned to the FMA” by the provisions of the BWG and other relevant laws (Article 2, paragraph 1 of the FMABG and Article 69, paragraph 1 of the BWG), including AML/CFT provisions. In exercising its supervisory role, the FMA must consider the national economic interest in maintaining an efficient banking system and financial market stability (Article 69, Paragraph 1 of the BWG).

668. Since 2008, the OeNB conducts all onsite missions to banks upon the mandate of the FMA. AML/CFT issues are examined either by inspections for prudential requirements, or by focused missions. The number of OeNB missions including AML/CFT was about 35 on annual average over the past years, but less than a third of these inspections (11) were a comprehensive review of AML/CFT preventive measures. To augment these numbers further, the FMA made visits to bank management (“Company Visits”), 13 in 2007 and 14 in 2008 so far.

Statistical Table 26. Onsite Examinations of Credit Institutions

Mission Scope	Supervisory Body	2004	2005	2006	2007	2008
AML/CFT	OeNB	9	9	13	13	11
Prudential, incl. some AML/CFT	OeNB	25	32	20	14	28
	FMA	7	13	8	8	-

669. The number of full AML/CFT onsite examinations appears to be very low, compared to the number (871) of credit institutions which are under supervision. Some activities, such as exchange offices (12), have never been inspected. Although some examinations have been conducted outside Austria, relative numbers are low.

670. Domestic financial institutions are required to comply with BWG AML/CFT provisions, but the FMA is not in charge of their supervision. According to the provisions of the AVG (Articles 1 and 2), the local district authorities as the first instance and the governor in each of the *Land* as the second instance are in charge of ensuring compliance with the rules and regulations which “do not contain any provisions with regard to jurisdiction in the subject matter”, including in the case domestic financial institutions. No specific data were provided as to the type and scope of supervisory diligence. The authorities estimate that each one of the local district authorities conducts 10 to 50 on-site controls in all areas of activities (i.e., DNFBPs, see chapter 4) which are under its administration.

### Insurance Undertakings

671. Article 1, paragraph 1 of the FMABG empowers the FMA to supervise insurance activities. It involves “performing the official tasks and exercising the powers which are assigned to the FMA” by the provisions of the VAG and other relevant laws (Article 2, paragraph 2 of the FMABG). Pursuant to Article 99, paragraph 1 of the VAG, “the FMA shall, to the extent of the license granted (...), supervise all business practices of insurance undertakings, in particular the adherence to the provisions applicable to the obligation of the contractual insurance business.”

672. Article 104, paragraph 1 of the VAG constitutes the legal basis for the actions that the FMA may take in fulfilling its supervisory function, and, in its wording, clearly limits the purpose of these actions to the safeguard of “the interest of the insured.” The authorities referred the assessors to a decision of the Supreme Administrative Court<sup>35</sup> which rules that, when applying Article 104, paragraph 1 of the VAG, the authority is obliged to safeguard also the “principles of the due operation of private insurance companies.” As regards to infringements of AML/CFT provisions, Article 108a, paragraph 1, no. 2 gives the FMA power to sanction those as administrative offenses.

673. A level of supervisory effectiveness is demonstrated in the onsite examinations undertaken by the FMA which conducted three inspections to insurance undertakings during 2008 that were specifically focused on AML/CFT, but no other more general examinations or management visits. Two inspections were performed in 2007 and in 2006 respectively, in addition to, correspondingly, one and three company visits. No proceedings were taken against firms. Considering the size of the insurance business in Austria, 31 life insurance undertakings (and 51 non life insurance undertakings), the AML/CFT onsite supervisory process need to be expanded further.

### **Securities Institutions**

674. Supervision by the FMA of investment firms and investment services undertakings is based on Article 1 of the FMABG and Article 91 of the WAG, and involves “performing the official tasks and exercising the powers which are assigned to the FMA” by the relevant laws, among which the WAG (Article 2, paragraph 3 of the FMABG). The WAG specifically mentions that “the FMA shall control compliance with [the WAG]” (Article 91, paragraph 1 WAG), and in doing so, includes the monitoring of compliance with the AML/CFT provisions set out in the BWG to which Articles 6 and 12, paragraph 4 of the WAG refer.

675. The FMA conducted 15 inspections to investment firms and investment services undertakings during 2008 that included AML/CFT elements, but no on-site inspections that were specifically focused on AML/CFT and no visits were made to the institutions’ management specifically for the purpose of discussing AML/CFT matters. No AML/CFT oriented actions were taken against investment businesses. Overall the number of inspections is low in comparison to the number of licensed investment firms, 308.

676. Supervisory authorities rely heavily on external auditors (certified public accountants) to examine all other financial institutions, and seek confirmation that AML/CFT controls are in place and operational. Certified public accountants are subject to a professional code of conduct and follow auditing guidelines published by their professional association. The FMA has the power to reject and rescind the appointment of an auditor (Article 60 of the BWG and Article 82 of the VAG). The structure and the content of the annex to the audit report on the annual financial statements are laid down in a regulation (*Verordnung über die Anlage zum Prüfbericht*). External auditors must complete checks following a prescribed checklist which address most of the AML/CFT provisions. The AML/CFT system must be included in the audit review of insurance undertakings (Article 82,

---

<sup>35</sup> Decision GZ AW2008/17/0004, dated March 11, 2008.

paragraph 6 of the VAG), although there is no checklist for external auditors of insurance undertakings. Similar provisions are in place for securities institutions (Article 93 of the WAG).

677. The increasing trend in examination numbers, plus meetings with senior management, demonstrate the OeNB and FMA are taking steps to ensure supervision is being carried out and indeed, particularly in the credit institutions, the law is being enforced. Additional efforts—and resources—are required to further extend the number of on-site missions focusing on ML/FT risks.

678. The FMA and the OeNB have developed a risk-based approach to supervision. Every on-site mission, with the exception of market model validation, includes an AML/CFT examination, which focuses on systems and procedures in the context of a general inspection, and extends to customer file and transaction sampling in the context of a targeted AML/CFT examination. The OeNB and FMA have access to a risk rating model and both contribute to it. The model includes assessment of all risks an institution may face, including operational risks which in turn includes AML/CFT risk. AML/CFT has a low-risk weighting in the model, but the analyst can increase this weighting on the basis of information collected from various sources. As a result, some banks with high nonresident deposits, notably those located in Jungholz and Mittelberg, have been subject to on-site examinations. However, the size of the business is a major factor when determining priorities for examinations, although it may not be fully relevant for some ML/FT typologies. Thus, none of the 12 independent *bureaux de change* has ever been examined for AML/CFT compliance on the basis that turnover is low, while such activities are generally considered as particularly exposed to ML/FT risks.<sup>36</sup>

679. The eight banks which are of systemic importance are examined on annual basis, while second tier banks are inspected every two years. Other institutions are subject to onsite examination where offsite analysis, external auditors' reports or other sources raise concerns. The authorities should consider putting resources in place to enable insurance and investment supervisors to raise the focus of their on-site work to assess these regulated entities' compliance with their AML/CFT, and to step up AML/CFT examinations of credit and domestic financial institutions. It is particularly important given the useful safeguard of the external auditor checklist does not apply other than to credit institutions.

***Fit and Proper Criteria and Prevention of Criminals from Controlling Institutions (c. 23.3 & 23.3.1):***

**Credit Institutions**

680. Pursuant to Article 5, paragraph 1, no. 6 of the BWG, a number of conditions must be met before the FMA may issue the requested license, among which the absence of “reasons for exclusion as specified in Article 13, paragraphs 1, 2, 3, 5, and 6 of the Trade Act of 1994.” The reasons for exclusion are as follows:

- (1) instances where the applicants, for example entity that wishes to be regulated, the members of its management board, or chairman of its supervisory board (Article 28a, paragraph 3 of the BWG):

---

<sup>36</sup> Foreign exchange transactions are listed among banking activities and also conducted by commercial banks.

1. have been sentenced by any court
    - a) for certain offenses such as fraudulently withholding payment of social insurance contributions, fraudulent bankruptcy, damage to creditors, preference of any creditor, or grossly negligent injury to any creditors' interests, or
    - b) for any other criminal offense to a term of imprisonment of more than three months or a fine of more than 180 daily rates,
  2. and the sentence has not yet been removed from the criminal record.
- (2) Whoever has been sentenced by any fiscal prosecution authority for having committed fiscal offenses such as smuggling, evasion of import or export taxes, handling of smuggled goods, is also to be excluded from carrying on any trade or business, and therefore from being granted a license by the FMA, if he or she has been sentenced to a fine of more than EUR 726, or to both a fine and a term of imprisonment, and if no more than five years have elapsed since sentencing.
- (3) Legal entities must also be excluded from carrying on any trade or business, and consequently from being granted a license by the FMA,
1. if, for presumed lack of sufficient assets to cover the cost of bankruptcy proceedings, such proceedings have not been instituted or have been discontinued, and
  2. if the period of access to the insolvency case referred to above in the insolvency database has not yet elapsed.
- (4) A natural person shall be excluded from carrying on any trade or business if this person has or had substantial influence on the conduct of business operations of a legal entity other than a natural person which is or was excluded from carrying on any trade or business under paragraph 3. If any of the grounds for exclusion referred to in paragraph 4 applies to the legal entity, the natural person shall only be excluded from carrying on any trade or business involving activities of insurance mediation.
- (5) After having been deprived by court sentence of the right of carrying on a trade or business, or after having suffered withdrawal of one's trade or business license under Article 87(1)3 or 4, a natural person shall be excluded from carrying on any trade or business if the performance of such a trade or business activity could frustrate the purposes underlying deprivation by court sentence or withdrawal under Article 87(1)3 or 4. This shall also apply to any natural person who has occasioned official measures under Article 91(1) or (2) for any of the reasons of withdrawal referred to in Article 87(1)3 or 4.

681. Article 28a, paragraph 3 of the BWG establishes special additional requirements for the chairpersons of the supervisory boards in large credit institutions (total assets exceeding EUR 750 million), notably that:

- no bankruptcy proceedings have been initiated for their assets or any entity other than a natural person on whose business the chairpersons of the supervisory board have or have had a decisive influence;

- the chairpersons find themselves in an orderly economic situation and no facts are known which would raise doubts as to their personal reliability; and
- the chairpersons possess the professional qualifications and experience necessary for performing their function; such professional qualifications require expertise in the fields of bank finance and accounting as appropriate to the credit institution in question.

682. Similarly, Article 5, paragraph 1, no. 7 of the BWG requires directors (management board members) to be “in an orderly economic situation” and that their personal reliability is not subject to any doubt. Pursuant to Article 5, paragraph 1, no. 3 of the BWG, a license can be issued when no facts are known which would raise doubts as to the personal reliability of the persons who hold qualifying participations who also must ensure sound and prudent management of the credit institution. A qualifying participation is defined in Article 2, paragraph 3 of the BWG, as a direct or indirect participation (i) which represents 10 percent or more of the capital or voting rights or (ii) which makes it possible to exercise significant influence over the management. The FMA must be notified in advance of any intended change in parties holding qualifying participations (Article 20, paragraphs 1, 2, and 5 of the BWG), and, at least once a year, of the names, addresses and holdings of qualifying participation holders. However, the option for credit institutions to issue bearer shares appears to be a major impediment to FMA monitoring of significant or controlling interests.

683. There are no provisions which apply to members of the supervisory board or to senior managers (apart from the above-mentioned provisions for board chairpersons). In the latter case, the authorities point to Article 39 of the BWG which defines general due diligence obligations for credit institutions which, in their view, include risks arising from hiring unqualified or unsuitable employees. However, c. 23.3.1 explicitly requires supervisors to evaluate senior managers on the basis of fit and proper criteria.

684. Assessors were informed that a full fit and proper assessment was made with regard to shareholders and members of the management board of credit institutions and chairmen of supervisory boards which included:

- receipt of a police certificate confirming no criminal convictions;
- checking qualifications/memberships claimed were indeed held;
- taking up references from previous employers to check experience claimed;
- taking up regulatory references from other regulators or other supervisory bodies within Austria or internationally.

### **Domestic Financial Institutions**

685. These institutions are subject to the general provisions of the GewO, which do not adequately cover the requirements of c.23.3 and c.23.3.1 for financial institutions. Pursuant to Article 13 of the BWG, prior insolvency is the only cause prohibiting legal entities or natural persons from carrying on their business. An additional cause is for natural persons to carry to have committed a criminal offense and been sentenced by a court to a term of imprisonment of more than three months or a fine exceeding 180 daily rates (Article 13, paragraph 1 of the GewO). Also, a managing director has to be

appointed if the applicant fails to prove his qualifications (Article 16, paragraph 1 of the GewO). These provisions fall short of meeting the licensing requirements defined by the criteria.

### **Insurance Undertakings**

686. Pursuant to Article 11a, paragraphs 3 and 5 of the VAG, the chairperson of the supervisory board of an insurance company with premium written of all business activities exceed EUR 500 million is subject to specific fit and proper requirements. Under Article 4, paragraph 6, no. 1 of the VAG, the FMA is prohibited from granting a license if the members of the management board or the administrative board or the managing directors of an insurance company do not have the required personal reliability and professional qualifications to fulfill their duties. The law specifies that “at any rate, the conditions of personal reliability shall not be deemed fulfilled if there is a ground for exclusion as defined in Article 13 of the GewO” described above. During the licensing process, the FMA must therefore establish the personal reliability of board members and managing directors, but not necessarily other senior managers as required under the standard.

687. Pursuant to Article 4, paragraph 6, no. 5 of the VAG, a license shall not be granted to persons who, holding direct or indirect participating interests of at least 10 per cent of the share capital or of the voting rights or exerting a decisive influence on the management in any other way, do not ensure a sound and prudent management of the insurance undertaking. The FMA must be notified immediately of such changes in equity interests (Article 11b, paragraph 1 of the VAG.), and be informed at least once a year of the names and addresses of those shareholders as well as the extent of their equity holdings. It shall prohibit those equity transactions when licensing requirements are not met. As for credit institutions, bearer share holdings restrict FMA’s ability to monitor significant or controlling interests.

### **Securities Institutions**

688. Before granting a license under the WAG, the FMA must establish that a number of conditions have been fulfilled, and must satisfy itself that “due to their qualifications, managers (...) are suitably qualified and have the skills and experiences required for providing investment services” (Article 3, paragraph 5, no. 3 WAG). Under criteria listed in Article 10, paragraph 1, managers (i.e., members of the management board) must be of “sufficiently good repute” and sufficiently experienced. In addition, licensing requirements in Article 5 of the BWG must also be met. The criteria for selection do not apply to supervisory board members and to senior managers.

689. Changes and amounts in qualified holdings must be notified to the FMA, together with the identities of shareholders, whether direct or indirect, natural or legal persons (Article 11, paragraphs 1 and 2 of the WAG). Pursuant to Article 11, paragraph 6 of the WAG, the FMA shall take appropriate measures where the influence of qualified shareholders “is likely to be prejudicial to the sound and prudent management” of the securities institution. The identification of persons possessing qualified holdings is also subject to the limitations inherent to bearer shares.

### ***Application of Prudential Regulations to AML/CFT (c. 23.4)***

690. Both FMA and OeNB apply their full range of prudential regulation to AML/CFT matters where is it appropriate to do so. For example, with regard to licensing and structure, Article 4,

paragraph 3, no. 5 of the BWG and Article 11, paragraph 1 of the WAG require applicants to disclose the identity and shareholdings of owners over a certain percentage, indicate group structure and disclose information relating to the reliability of owners and directors. Additionally, Article 5, paragraph 1, nos. 3 and 4 of the BWG and Article 3, paragraphs 5 and 6 of the WAG require that shareholders meet appropriate standards (namely the fit and proper test). The VAG has similar provisions with the addition in Article 4, paragraph 6, nos. 5 and 7 that the license must not be granted if there is a lack of transparency in the group structure, or if the FMA cannot fulfill its duties or if granting the license would be contrary to the interests of policy holders.

691. Further examples of prudential regulation being applied for AML/CFT purposes would include all license holders being required to have adequate risk management processes in place. The FMA and the legislative framework place a high degree of importance on firstly the obligation to establish a robust risk management framework (which includes specifically ML/FT risks), but also then the obligation to have an internal audit function to check the efficacy of the risk management controls. Ongoing supervision includes specific on site review of AML/CFT procedures and meetings with senior management regarding AML/CFT matters.

***Licensing or Registration of Value Transfer/Exchange Services (c. 23.5) & Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6)***

692. “Remittance services business” is defined under Article 1, paragraph 1, no. 23 of the BWG as “the transfer of funds, except for physical transports, by accepting money or other means of payment from the originator and paying out corresponding amount in money or other means of payment to the beneficiary by way of non-cash transfer, communication, credit transfer or other uses of a payment or clearing system.” It is a type of “banking transactions” subject to licensing by the FMA (Article 1, paragraph 1 and Article 4 of the BWG). Money and value remitters are therefore considered as “credit institutions” under Austrian law and, as such, are subject to AML/CFT supervision by the FMA. All measures relating to licensing and prudential supervision apply to these businesses including specific AML/CFT on site assessment as outlined above.

693. Money and currency exchange business are defined as banking transactions which, as such, can only be conducted by credit institutions, once they have applied for and been granted the necessary license by the FMA (Article 1, paragraph 1, no. 22 and Article 4 of the BWG). Like money remitters, stand-alone *bureaux de change* are subject to the FMA’s supervision, including for AML/CFT purposes. It is understood that although the full range of offsite provisions apply to this sector, examinations have not been conducted yet; supervisors classify those activities as low ML/FT risk because their volume of activity is considered small (currency exchange activities which are conducted by commercial banks are including in the supervisory review of those institutions).

***Licensing and AML/CFT Supervision of other Financial Institutions (c. 23.7)***

694. As mentioned above, the Austrian definition of credit institutions and financial institutions according to Article 1, paragraph 2 of the BWG is extremely wide. Assessors have not identified financial institutions covered by the Core Principles which are not included in the FMA’s AML/CFT prudential and conduct of business oversight.

***Guidelines for Financial Institutions (c. 25.1)***

695. The FMA has taken the approach of issuing guidance in the form of circulars (*Rundschreiben*). Although not legally binding they contain interpretation of the provisions in the various regulatory laws and suggestions as to good practices. The authorities informed the assessors that, in some cases, lack of knowledge of the administrative law violated may be an excuse (Article 5, paragraph 1 of the Administrative Penal Act (*Verwaltungsstrafverfahrensgesetz, VStG*)), leading to closure of the case. Clarification and interpretation of the law provided by circulars are made available to the public on the FMA website. They have therefore major legal implication, as a failure to comply with a circular is a failure to comply with the law and will be sanctioned for breach of the law.

696. Circulars have been issued for all financial institutions of the industry (credit institutions, insurance undertakings and securities institutions). However, four circulars which were published from 2003 to 2006 need revision and update in response to the significant upgrading of the AML/CFT framework in January of this year:

- an updated Circular on Identification and Verification of Identity was issued on July 3, 2008 and had just been made available to the financial institutions at the time of the mission; and
- a *Rundschreiben der FMA zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen* (-revised- Circular on Identification and Verification of Identity for Insurance Undertakings) was published on November 14, 2008 (only in German).

697. Three additional circulars are being prepared, and will be issued after consultation with the industry. Until the updated circulars are distributed, however, industry is having to implement the new legal provisions without regulatory guidance, although the revised laws introduce substantial additional requirements for identification requirements, risk-based approach, and higher risk customers.<sup>37</sup> In addition, guidance provided by exiting circulars is somehow limited as, in some cases, circulars refer to provisions which have been repealed. The authorities mention that credit institutions can, at any time, require clarification from the FMA.

698. The Division Bank and Insurance<sup>38</sup> of the WKO, acting as a professional body, may also prepare guidelines for its members, which it did a few years ago, before AML/CFT legal provisions were issued.

699. Typology work is not carried out by the FMA to any significant extent as this is felt to be a matter falling more to the A-FIU skill set.

### ***Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1)***

#### **Credit Institutions**

---

<sup>37</sup> At the time of the assessment, over nine months had elapsed since the introduction of the amendments to the laws.

<sup>38</sup> Including securities firms.

700. Pursuant to Article 69, paragraph 1 of the BWG, the FMA must monitor compliance with the provisions of the BWG and other relevant laws by credit institutions which carry out activities in Austria. The law further provides that the FMA must, in consideration of the nature, scope and complexity of the banking transactions, monitor, among other elements, the qualitative coverage of all material risks from banking transactions and banking operations (Article 69, paragraph 2 of the BWG).

701. To the effect of monitoring compliance, the FMA may:

- request credit institutions according to Article 1, paragraph 2 of the BWG to provide interim financial statements, reports in specified forms, audit reports and information on all business matters;
- request audit reports and information from the bank auditors;
- instruct bank auditors of credit institutions or other experts to conduct all necessary audits; and
- instruct the OeNB to conduct audits of the credit institutions (Article 70, paragraph 1, nos. 1 to 4 of the BWG).

702. Assessors saw evidence of these provisions being regularly applied with good levels of off-site monitoring, for example, via the external auditor checklist, and a regular program of on-site examinations relating to general controls (including AML/CFT matters), examinations specifically focusing on AML/CFT matters and a series of meetings with senior management. Following these various supervisory methods, enforcement actions with regard to AML/CFT weaknesses have been taken (see write-up for Recommendation 17 below).

### **Domestic Financial Institutions**

703. The local district authorities are in charge of ensuring compliance of those institutions with the BWG. For lack of provision addressing the supervision of domestic financial institutions in the BWG, the investigation procedures defined in Article 37 to 38a of the AVG apply. The local district authorities shall process “any submission, application, information laid against somebody, complaints and other reports” (Article 13, paragraph 1 of the AVG), or may act *ex officio*, and launch an investigation procedure to ascertain relevant facts and to enable the parties to claim their rights and legal interests (Article 37 of the AVG).

### **Insurance Undertakings**

704. In order to ensure the legitimacy of the insurance business, the FMA may—also with regard to the insurance intermediaries—at any time request information and the submission of documents, as well as carry out on-site inspections (Article 100, paragraphs 3 and 101 of the VAG).

705. Assessors saw evidence of comprehensive desk based supervision of the insurance sector and some evidence of onsite work. The FMA conducted three inspections to insurance undertakings during 2008 that were specifically focused on AML/CFT, but no other more general examinations or management visits. No proceedings were taken against firms.

### **Securities Institutions**

706. When exercising its supervisory functions of the investment firms and investment services companies, the FMA is, at any time, authorized:

- to access records, documents and durable medium of the companies;
- to request information from the companies and to summon and question persons;
- to carry out audits on-site using its own auditors or other experts;
- to request existing records of telephone calls and data transmission;
- if the licensing conditions are no longer met or if a legal entity or its managing directors are in breach of other relevant provisions, instruct the entity or its directors to restore legal compliance within a specific period of time; in case of repeated or continued violations, completely prohibit directors from managing the company, or; revoke the license;
- to apply for injunctive relief with the competent prosecution authorities pursuant to Article 144a of the StPO;
- to request information from auditors and statutory audit institutions;
- to demand the suspension of trading in any financial instrument by a listed company and a Multilateral Trading Facility;
- to demand the revocation of the registration of any financial instrument by way of regulatory measures; and
- to report any suspicion of punishable acts to the prosecuting authorities or security authorities (Article 91, paragraph 3 WAG).

707. As previously reported, assessors saw evidence of regular inspections to investment firms and investment services undertakings during 2008 that included AML/CFT elements, but no on-site inspections that were specifically focused on AML/CFT. Further, no visits were made to investment firms/services management specifically for the purpose of discussing AML matters. No AML/CFT oriented actions were taken against investment businesses.

#### ***Authority to conduct AML/CFT Inspections by Supervisors (c. 29.2):***

### **Credit Institutions**

708. The FMA may instruct the OeNB to conduct audits of:

- credit institutions;
- their branches and representative offices outside Austria;
- credit institutions which are subject to supplementary supervision pursuant to Article 5, paragraph 11 of the Financial Conglomerates Act; and
- undertakings within the group of credit institutions (Article 70, paragraph 1, no. 3 of the BWG).

709. The FMA mandates the OeNB to carry out on-site inspection work of credit institutions. To determine which institutions shall be visited an annual plan is drawn up and agreed between the two regulatory authorities. The key tool in supporting this planning process is a risk model built up from information gleaned from a number of sources including:

- The desk based work done by the FMA in relation to examining applications, organization and business plans, compliance and operational manuals and audited statements (including the external auditors' checklists which specifically include the strength of AML/CFT controls);
- The offsite monitoring and onsite examination done by the OeNB in relation to reviewing policies, procedures, books and records, and sample testing to ensure institutions evidence that these systems are implemented in practice. The OeNB has conducted more narrowly scoped onsite examinations focusing on AML/CFT matters. These examinations concentrate on account opening procedures, customer due diligence, the risk based approach, account monitoring and reporting obligations; and
- The OeNB also pays close attention to the solvency and liquidity matters relating to bank capital requirements and must understand the various risks faced by banks and their means of managing them, in order to evaluate the capital adequacy requirements under the various Basel standards. This work while focusing on prudential regulation objectives includes assessing AML/CFT risks and the control environment in place to manage them.

In addition, the FMA can at any time request the OeNB to conduct additional inspections.

### **Domestic Financial Institutions**

710. The AVG contains also detailed rules of procedure, which apply to an investigatory process, following a request or complaint. The purpose of the investigation procedure, essentially in form of oral hearings, is "to ascertain the state of facts... and to enable the parties to claim their rights and legal interests" (Article 37 of the AVG). It is not clear to the assessors that such general procedures would be adequate to ensure domestic financial institutions' compliance with the AML/CFT provisions of the BWG. No evidence has been presented of an effective AML/CFT supervision of domestic financial institutions.

### **Insurance Companies**

711. The FMA may conduct on-site inspections of the business practices of insurance undertakings at any time (Article 100, paragraph 3 and Article 101, paragraph 1 of the VAG). This also applies to undertakings to which parts of the business activities have been transferred (Article 101, paragraph 2). If it is necessary, the FMA may also appoint inspectors who are not part of the FMA (Article 101, paragraph 3 of the VAG).

712. As previously outlined, no general systems and controls examination have been conducted in the insurance sector. However, three specific AML/CFT focused examinations were undertaken and these concentrated on account opening procedures, customer due diligence, the risk based approach, account monitoring and reporting obligations.

### **Securities Institutions**

713. As mentioned above, the FMA is entitled to conduct onsite inspections of investment companies and investment services companies (Article 91, paragraph 3, no. 3 of the WAG). FMA staff require a substantial amount of information is submitted as part of the on-site examination preparation process. Prior to the examination, supervisors review the organization chart, business plan, policies, procedures, training and compliance manuals of an institution and move on-site with a good overview of the activity of the business and likely risks or weaknesses it faces. The examination would then focus on looking at books and records, and sample testing to ensure institutions evidence that their systems, policies and procedures are implemented in practice. Particular attention is paid to account opening procedures, customer due diligence, the risk based approach, account monitoring and reporting obligations.

***Power for Supervisors to Compel Production of Records (c. 29.3 & 29.3.1)***

714. As mentioned in the write-up of criterion 23.1 above, the FMA may, in all three sectors that it supervises, compel production of or have access to all documents relevant to monitoring compliance with the AML/CFT requirements. The FMA may exercise this right on its own accord, without the need to apply for a court order. Assessors heard evidence of regular exercise of these powers.

715. Financial institutions files STRs with the A-FIU. When analysis of an STR leads the A-FIU to consider that a financial institution is in breach of the AML/CFT legislation, it forwards the case to the FMA who may initiate proceedings.

716. For domestic financial institutions, the local district authorities can summon persons which residence is within its territorial jurisdiction when deemed necessary (Article 19 of the AVG). The procedure does not provide for onsite examinations, nor for access to internal record and documents of a domestic financial institution.

***Powers of Enforcement & Sanction (c. 29.4)***

717. The FMA may take measures under the general supervisory regime and the Administrative Penal Act (VStG) in order to restore legal compliance. Enforcement measures and sanctions can be imposed on:

- Legal persons: under the supervisory regime, credit institutions, insurance undertakings and securities business can be fined up to EUR 30,000; the next and ultimate sanction would be loosing their license and closing their business.
- Natural persons:
  - under the supervisory regime, management board members of a credit institution or a securities business may be restricted or prohibited from managing such entities;
  - under the VStG, management board members of credit institutions, insurance undertakings and securities business who are responsible for a violation of AML/CFT

requirements can be sanctioned with a fine up to EUR 30,000,<sup>39</sup> unless the act constitutes a criminal offense subject to Criminal Court rulings.

718. The sanctioning regime does not apply to financial institutions' supervisory board members or senior managers.

*Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1); Designation of Authority to Impose Sanctions (c. 17.2); Ability to Sanction Directors & Senior Management of Financial Institutions (c. 17.3); Range of Sanctions—Scope and Proportionality (c. 17.4)*

### **Credit Institutions**

719. The FMA is entitled to address non-compliance with the AML/CFT provisions through two different sanctioning regimes, as outlined above:

- measures under the supervisory system (Article 70 of the BWG); and
- measures under the VStG (Articles 98 and 99 of the BWG).

720. **Measures under the supervisory regime** may be taken in accordance with Article 70, paragraph 4 of the BWG. When a credit institution violates the provisions of the BWG (or other relevant laws), including AML/CFT preventive measures, the FMA may:

- instruct the credit institution on pain of penalties (up to EUR 30,000) to restore legal compliance within a certain period of time;
- in case of repeated or continued violations, enforce the penalty and reiterate the instructions above-mentioned on a higher penalty, or completely or partly prohibit the directors from managing the credit institutions;
- revoke the license when other measures under the BWG cannot ensure the functioning of the credit institution.

721. Before issuing orders on pain of penalties, the FMA can instruct credit institutions to provide comments or to report within a certain timeframe on deficiencies, and additional investigations can be conducted.

Statistical Table 27. Supervisory Actions related to AML/CFT Infringements

	2006	2007	2008
<b>Comments required from financial institutions under administrative procedure law</b>	na	21	2
<b>Reporting obligations under administrative procedure law</b>	na	3	-
<b>Further investigations under administrative procedure law</b>	na	1	25

<sup>39</sup> The FMA has postulated an increase of the amount of administrative fines.

722. The authorities declare that instructions under threat of penalty proved generally to be sufficient, and that enforcing the sanction and repeating the order are infrequent: only seven cases -all related to repeated infringements of prudential provisions- have been sanctioned in 2003 and 2004. There have been no cases where members of the management board were prohibited of conducting business, or license was revoked.

723. These types of actions may be rendered public, but instructions to restore legal compliance should only be published if this is necessary for the purpose of informing the public and in light of the nature and the severity of the violation (Article 70, paragraph 7 of the BWG). Pursuant to Article 22, paragraph 1 of the FMABG, the FMA is competent to enforce its administrative rulings and can impose a monetary fine of up to EUR 30,000. Appeals against these actions are not permissible (Article 22 FMABG), but they may be subject to review by the Austrian Administrative Court and/or the Austrian Constitutional Court.

724. **Sanctions of administrative penal procedure** (Article 98, paragraph 2, no. 6 and Article 99, no. 8 of the BWG; Article 108a, paragraph 1, no. 2 of the VAG): Violations of AML/CFT preventive measures set forth under Article 40, 40a, 40b and 41 Paragraphs 1 to 4 of the BWG by persons responsible for a credit institution may also be punishable with a fine of up to EUR 30,000. The penalty must be based on the extent of damage resulting from the offense or the danger it causes to the interests to be protected by the sanction, and to what extent the offense resulted in further detrimental consequences. Aggravating or mitigating circumstances have to be considered and special emphasis must be laid on the degree of the guilt (Article 19, paragraph 1 of the VStG). The authority responsible for the issuance of administrative penal sanctions is the FMA (Article 22 of the FMABG), but enforcement of these orders is of the competence of the local district authorities, on the basis of the VStG. The available statistics on administrative penal proceedings show a sharp increase in actions, but rare convictions and a low level of fines.

Statistical Table 28. Administrative Criminal Actions for AML/CFT cases: number and fines

	2007	2008
<b>Proceedings</b>	9	27
<b>Out of which: - dispensed</b>	6	25
	1 (EUR 6,000)	1 (EUR 4,000)
<b>- sanctioned</b>	1 (EUR 8,000)	1 (EUR 4,000)
	1 (EUR 12,000)	-

725. In case of multiple offenses, sanctions can be imposed cumulatively. No such case has been mentioned to the assessors.

726. In administrative penal proceedings for violation of the law, the defendant's personal guilt must be established. Negligence, which may automatically be assumed in case of a violation of AML/CFT preventive measures (Article 5, paragraph 1 of the VStG), constitutes liability for punishment. The lack of knowledge of the provision of the administrative law violated may be an excuse for the violation, if proven to be without the culprit's fault and "if he was not able to realize the illicit character of his doing without knowing the respective provision of the administrative law" (Article 5, paragraph 2 of the VStG). Circulars are published on the FMA website and the persons

responsible for the supervised undertakings (Article 9 of the VStG) can easily familiarize themselves with all relevant provisions. The authorities point to the fact that the Administrative Court follows a very strict interpretation of Article 5, paragraph 2 VStG.

727. These measures are without prejudice to Criminal Court applying the StGB sanctioning provisions related to the criminal offenses of ML/FT. For legal persons and entities, the Austrian Federal Statute on the Responsibility of Entities for Criminal Offenses (*Verbandsverantwortlichkeitsgesetz, VbVG*) provides a general criminal liability for legal persons and entities for all penal offenses, including ML/FT. The jurisdiction over legal persons and entities for the underlying offense follows the general rule of the StGB for territorial and nationality based jurisdiction, as it is stipulated for natural persons.

### **Domestic Financial Institutions**

728. Article 99, paragraph 8 states that the person responsible for a domestic financial institution who violates the BWG provisions related to AML/CFT is guilty of an administrative offense and may be sanctioned by the FMA with a fine up to EUR 30,000. Until now, no sanction has been issued against a person responsible for a domestic financial institution. There is no provision for taking sanctions against a domestic financial institution itself.

### **Insurance Undertakings**

729. Pursuant to Article 108a, paragraph 1, no. 2 of the VAG, violations of AML/CFT provisions constitute an administrative offense for which the FMA must issue fines up to EUR 30,000. In addition, the license shall be revoked if the insurance undertaking seriously violates its obligations stated in the VAG (Article 7b, paragraph 1, no. 3 of the VAG). No sanction has been issued for infringement of AML/CFT provisions.

### **Securities Institutions**

730. Article 92, paragraph 8 of the WAG empowers the FMA to take measures under the supervisory regime defined in Article 70, paragraph 4 of the BWG against a legal entity which is not in compliance with the provisions of the WAG. Pursuant to Article 94, paragraph 8 of the WAG, a manager of a legal entity which is in violation of the AML/CFT provisions, defined in the BWG, commits an administrative criminal offense and is subject to a EUR 30,000 fine. The FMA has never issued a sanction for breach of AML/CFT rules.

731. Sanctioning powers for violating the AML/CFT provisions do not seem proportionate and dissuasive:

- a credit institution or a securities business only can be fined up to EUR 30,000, the other available sanction under the supervisory regime is revoking the license;
- management board members of a financial institution can be sanctioned with a fine up to EUR 30,000, under the VStG, unless the act constitutes a criminal offense subject to Criminal Court rulings; and
- management board members of a credit institution or a securities business may also be restricted or prohibited from managing such entities, under the supervisory regime.

732. The range of sanctioning provisions is limited under the supervisory regime, creating gaps which hinder the proportionality of sanctions. In addition, the level of maximum fines under both regimes is a very weak deterrent.<sup>40</sup> The low amount of fines effectively issued lessens further the dissuasive effect of the system.

733. Pursuant to Article 70, paragraph 4, no. 7 of the BWG, the FMA is entitled to make public its supervisory actions, in full or in part, but, as regards to orders and penalties, “in light of the nature and severity of the violation.” In practice, supervisory sanctions are not disclosed.

***Adequacy of Resources for Competent Authorities (c. 30.1)***

**Structure and Independence**

734. The FMA is an autonomous institution under public law which is placed under parliamentary control. Article 3 of the FMABG deals with the Federal Government liability for “damage caused by the FMA’s bodies and employees” when performing their official duties. Pursuant to the Public Liability Act (AHG), the government may be sued for even slight negligence in supervision, and according to Article 3, paragraph 3, it is entitled to demand reimbursement from FMA’s bodies or employees. An amendment to the AHG passed on October 27, 2008, limits Government’s liability to damages that were directly caused to the legal entity subject to supervision. No case related to AML/CFT supervision has been brought to the courts so far.

735. The FMA appears to be structured in a manner that does not undermine its independence. While there is a tradition of working closely with industry and it was noted that two FMA board members are nominated by industry representative bodies, assessors did not sense that industry members interfere with the ability of the FMA to execute its functions independently. Similarly, the FMA appears to enjoy good, collaborative working relations with the OeNB and other government bodies such as MoI and their agencies, without any undermining of independence.

736. The structure however is such that it requires a high degree of coordination, with some divisions and departments having vertical responsibilities and others, cross divisional duties. The ML Competence Center is making a strong contribution to the AML/CFT skills development within the FMA, as a unit providing support and assistance to supervisory departments. There is also a higher level, interagency Task Force which meets quarterly and a high level Markets Group that considers key strategic issues at national level.

737. The AML Competence Center which is part of the International Affairs and European Integration Division, within the Department in charge of Integrated Supervision, is a policy and support function, rather than an operational unit. The authorities consider that the Center is in charge of formulating and driving the FMA AML/CFT strategy: it does so when representing the FMA in international and national working groups (including the Financial Market Committee), and spreading knowledge across the FMA.

---

<sup>40</sup> However, the Austrian Constitutional Court ruled that severe penalties can only be applied by Courts.

738. The consequence of this approach however may be that more than nine months after the introduction of significantly raised AML/CFT standards, industry still has no updated sets of guidance. The authorities underscore the possibility for financial institutions to contact the FMA in order to obtain clarification on legal provisions.

739. Views on where the key AML/CFT risks lie (both in the minds of regulators and industry) are still relatively unformed, and practical typologies relevant to the risks faced by the sectors are needed.

### **Resources**

740. Technical competencies within the FMA and OeNB are good. However, since 2005, staff turnover in the FMA has been increasing and remains high: 10.6 percent in 2005, 13.4 percent in 2006 and 13.9 percent in 2007, and many teams are young and appear relatively inexperienced. The gap between the number of positions budgeted and positions filled within the FMA is widening, from 4 percent in 2005 to 8 percent in 2007, and staffing levels are not sufficient at current numbers. This has already been identified by management and a program of recruitment is underway, which aims at increasing the workforce by 40 percent in the FMA. The OeNB plans also to augment substantially its staff, notably augment the number of onsite supervisors from 45 to 70 by 2010.

741. Assessors were interested in industry views on this topic and it was clear that while the OeNB and FMA both had the respect of the industry, the FMA teams were considered less experienced. Industry are aware a recruitment phase is underway but expressed mixed views as to the likelihood of the FMA attracting appropriate, experienced, staff. Assessors were informed that the market is competitive and that good risk management and compliance people are at a premium.

742. Pursuant to Article 19, paragraph 4 of the FMABG, the FMA is financed in part by the Federal Government budget (EUR 3.5 million). The remaining funding needs are charged to financial institutions subject to FMA supervision. OeNB is also entitled to recover some of its supervisory costs from banks. A lack of adequate funding should not be a barrier to the recruitment and retention of able and experienced staff. Technical support systems appear adequate.

743. The adequacy of local district authorities' resources for AML/CFT supervision of domestic financial institutions cannot be assessed.

### ***Integrity of Competent Authorities (c. 30.2)***

744. The staff at the FMA and OeNB appeared to assessors to have the highest integrity and the organizations demonstrated good recruitment policies with good follow up practices.

### ***Training for Competent Authorities (c. 30.3)***

745. The combination of a relatively new regulator, young staff and new laws, together with an industry expanding into new markets sets the scene for an organization (and indeed industry) with high training and development needs.

746. The initiatives within the FMA Academy are a good start in this area, but consideration should also be given to:

- short term secondments to regulatory bodies with established AML/CFT oversight program;
- medium term secondments or consultancy appointments to bring in the experience needed in the short term;
- recruitment policies that will focus on bringing in relevant AML/CFT practical experience, for example from other regulators, or those with forensic accountancy, police or compliance backgrounds.

***Statistics (applying R.32)***

747. The FMA keeps comprehensive records of supervisory actions related to AML/CFT. However, data related to domestic financial institutions are scarce.

**3.10.2 Recommendations and Comments**

748. Overall, the legal framework set out in the FMABG, BWG and the WAG adequately address AML/CFT monitoring and supervision, and provides the FMA with sufficient powers to conduct its functions. The sanctions that may be issued by the FMA do not appear to be proportionate and dissuasive; although the authorities stressed that the FMA scarcely has to make use of its sanctioning powers. For example, extending the range of approved persons beyond executive board level would provide a vital additional tool to prevent inappropriate persons gaining or remaining in employment within the finance sector. The authorities could also consider using its existing power to make public statements (reporting facts if names have to be suppressed) which are valuable for warning the public, educating the rest of the finance sector and enhancing transparency.

749. The authorities should:

**Recommendation 17**

- Make sanctions sufficiently proportionate and dissuasive;
- Extend sanctions under administrative criminal procedure to supervisory board and senior management members.

**Recommendation 23**

- Ensure that capital hold in form of bearer shares do not undermine the assessment of significant or controlling interest in a financial institution;
- Carry out fit and proper tests of senior managers and supervisory board members;
- Increase onsite examinations on AML/CFT compliance, as well as supervisory oversight of standards within branches and subsidiaries located abroad;
- Ensure that licensing requirements or other legal or regulatory measures would prevent criminals to control domestic financial institutions, and apply fit and proper test for their directors and senior managers.

**Recommendation 25**

- Develop additional guidance available to industry on the new legal requirements.

### **Recommendation 29**

- Establish a regime of supervisory sanctions for domestic financial institutions.

### **Recommendation 30**

- Provide resources, training and support sufficient to enable supervisory divisions to increase AML/CFT oversight.

#### **3.10.3 Compliance with Recommendations 17, 23, 25 & 29**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R.17</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Sanctions not sufficiently proportionate and dissuasive.</li> <li>• No sanctions for senior management besides sanctions for criminal liability.</li> <li>• Limited effectiveness.</li> </ul>
<b>R.23</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Assessment of significant or controlling interest in a financial institution undermined by capital hold in form of bearer shares.</li> <li>• Insufficient licensing requirements or other legal or regulatory measures which would prevent criminals to control domestic financial institutions, and lack of adequate fit and proper test for their directors and senior managers.</li> <li>• No requirements to carry out fit and proper tests of senior managers and supervisory board members in all types of financial institutions.</li> <li>• Low number of onsite examinations for AML/CFT compliance.</li> <li>• Effectiveness of AML/CFT supervision of domestic financial institutions was not established.</li> </ul>
<b>R.25</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Insufficient guidance available to industry on the new legal requirements.</li> </ul>
<b>R.29</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Low level of AML/CFT supervision of domestic financial institutions.</li> <li>• No supervisory powers of sanction against a domestic financial institution.</li> </ul>

### **3.11 Money or Value Transfer Services (SR.VI)**

#### **3.11.1 Description and Analysis**

##### **Legal Framework:**

750. Article 1, paragraph 123 of the BWG draws remittance services businesses into the definition of business that requires a banking license. Remittance services are defined as “the transfer of funds, except for physical transports, by accepting money or other means of payment from the originator and paying out a corresponding amount or other means of payment to the beneficiary by way of noncash transfer, communication, credit transfer or other uses of a payment or clearing system.”

##### ***Designation of Registration or Licensing Authority (c. VI.1)***

751. In this way, the Austrian FMA is empowered to require Money Value Transfer (MVT) service operators to be supervised under the BWG. The names, addresses of these licensed businesses are on the FMA website, together with details of the type of activity that they are authorized to conduct, along with all other regulated person’s details. Comments made above about deficiencies in the licensing process of credit institutions are also valid for MVT services.

##### ***Application of FATF Recommendations (applying R.4-11, 13-15 & 21-23, & SRI-IX)(c. VI.2)***

752. The full range of FATF recommendations apply to MVT service operators as to other institutions regulated under the BWG. Comments made above about weaknesses in the preventive measures for credit institutions are also valid for MVT services.

##### ***Monitoring of Value Transfer Service Operators (c. VI.3)***

753. Although the full regulatory oversight is applied to MVT service operators, the authorities have not made oversight of this area a priority in respect of their onsite visit program. Very limited meetings with the sector revealed generally good systems and an understanding of the risks involved in their business type. It was noteworthy that one firm in particular had submitted regular and significant numbers of STRs. Industry indicated they were aware that when customers were refused and blocked from future transaction services being made available to them, the customers would turn to unofficial, ethnic transfer systems to achieve their transfers. This opinion from a business well placed to understand the activities within its sector, together with associated comments made by the A-FIU, leads assessors to consider it would be prudent for both the FMA and A-FIU to increase their attention to the possibility of unauthorized activity in this area. Comments made above about weaknesses in the supervisory system for credit institutions are also valid for MVT services.

##### ***List of Agents (c. VI.4)***

754. Article 4(3)7 of the BWG requires banking license applicants (including MVT service operators) to include with their application the identify and address or place of establishing of all those natural or legal persons used by the credit institution outside of its place of establishment in the provision of remittance services (agents). Additionally, post application, license holders are required at Article 73 (1)14 to notify the FMA of any changes in the identity, address or place of incorporation of the agents details previously supplied.

***Sanctions (applying c. 17.1-17.4 in R.17)(c. VI.5)***

755. The regime of sanctions defined in the BWG applies to MVT. Comments made above about deficiencies in the sanctioning regime of credit institutions are also valid for MVT services.

**Effectiveness**

756. The authorities identified the risk of ML/FT stemming from informal money remittance systems and *hawala*. They therefore established a new unit within the FMA which is in charge of combating unauthorized banking business as of January 1, 2009, and notably identifying, sanctioning and bringing illegal/non-licensed transfer service operators under the regulatory regime.

***Applying Best Practices Paper for SR VI (c. VI.6)***

757. The full range of regulatory and legal sanctions that are available in respect of credit institutions and set out in detail at section 3 above, apply to MVT service operators, and exhibit the same deficiencies.

**3.11.2. Recommendations and Comments**

758. The authorities should revise the framework for preventive measures to address all deficiencies.

**3.11.3 Compliance with Special Recommendation VI**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>SR.VI</b>	<b>LC</b>	• Deficiencies in the framework for preventive measures.

**4. PREVENTIVE MEASURES—DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS**

759. In Austria, the preventive measures regarding DNFBPs can be found in the laws and regulations governing the respective businesses and professions. CDD measures have generally been in force since the implementation of Directive 2001/97/EC (Second EU AML Directive) adapting Directive 91/308/EEC (First EU AML Directive) and have recently been extended to new DNFBPs (TCSPs, traders in all kinds of goods), as well as refined in line with Directive 2005/60/EC (Third EU ML Directive).

760. The last amendments to the Lawyer's Act (*Rechtsanwaltsordnung, RAO*) and Notarial Code (*Notariatsordnung, NO*) became effective on December 29, 2007, amendments to the Trade Act (*Gewerbeordnung, GewO*) on February 2, 2008 and to the Directive on the Practice of Chartered Public Accountants and Tax Consultants Professions (*Wirtschaftstreuhandberufs-Ausübungsrichtlinie, WT-ARL*) and the Directive on the Practice of the Accountancy Professions (*Bilanzbuchhaltungs-(Berufs) Ausübungsrichtlinie, BiBu-ARL*) on April 23, 2008 and May 1, 2008. The Gambling Law (*Glücksspielgesetz, GSpG*) was enacted by the National Assembly (*Nationalrat*) on June 30, 2008. All those amendments were aimed at implementing the Third EU ML Directive into Austrian law.

761. The WT-ARL and the BiBu-ARL are based on Article 83, paragraph 2 of the Act on the Profession of Chartered public accountants and tax consultants (*Wirtschaftstreuhandberufsgesetz, WTBG*) and Article 69, paragraph 2 Accountancy Act (*Bilanzbuchhaltungsgesetz, BiBuG*) respectively and approved by the MoE. These Directives are regulations in the meaning of the Federal Constitutional Law (B-VG).

762. The following table indicates which DNFBPs are covered by AML/CFT provisions.

Statistical Table 29. Acts Implementing AML/CFT Measures for DNFBPs

FATF DNFBPs	Governing Act
Casinos	Gambling Law (GSpG)
Real estate agents	Trade Act (GewO)
Dealers in precious stones	Trade Act (GewO)
Dealers in precious metals	Trade Act (GewO)
Lawyers	Lawyer's Act (RAO)
Notaries	Notarial Code (NO)
Accountants	Directive concerning the Practice of the Chartered Public Accountants and Tax Consultants Professions (WT-ARL) and Directive concerning the Practice of the Accountancy Professions (BiBu-ARL)
TCSP (Business consultants)	Trade Act (GewO)

763. All non-financial businesses and professions designed by the FATF are covered by AML/CFT laws and regulations in Austria. There is still an issue of implementation with the law regarding TCSPs, as the authorities decided to subject to the AML/CFT provisions of the GewO only business consultants, which were only partially involved in the scope of activities defined as performed by TCSPs. In Austria, the Chamber of commerce defines business profiles for every activity and did not review the business profiles of the professions that used to provide trust and company services, in order to conform to the new legislation. The activity of providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements is devoted to two professions. The first is the profession of office services, consisting of writing, messenger services, receipt and forwarding of messages (*Büroarbeiten*). The second is the profession of office services consisting in the provision of office equipment and office facilities (*Büroservice*). At the time of the on-site visit, those two professions were performing TCSPs activities, in contradiction with the new AML/CFT provisions of the GewO.

764. Concerning casinos, AML/CFT provisions are provided by the Gambling Law (GSpG) in relation to games of chance that are subject to the game monopoly defined in Article 4 (1) GSpG. There are a significant number of card casinos that offer poker game. Poker game has been judged as a game of chance by the highest administrative court in 2005. MOF considers that they are illegal and has passed several indictments to the competent prosecution authorities for examination. An amendment to the GSpG is currently under preparation. Other casinos, called "gaming halls" are operating in Austria but are an exception to the monopoly, such as for slots machines if the amount of

the player's stake does not exceed EUR 0.50 and the prize does not exceed the amount of EUR 20 (Article 4 (2) GSpG). These casinos are under the supervision of local district authorities. All casinos activities outside the gaming monopoly are not subject to AML/CFT requirements.

765. Insurance intermediaries are regulated in the GewO, but applicable AML/CFT obligations are described in section 3. Since the GewO contains AML/CFT provisions for various DNFBPs (Real estate agents, dealers in precious metals and stones, and TCSPs), the reference to "tradespersons" is made to all professions covered by the GewO.

## **4.1 Customer Due Diligence and Record-keeping (R.12)**

### **4.1.1 Description and Analysis**

#### **Legal Framework**

##### **Casinos**

766. Customer due diligence and record-keeping requirements for casinos and electronic lotteries are regulated in the Gambling Law (GSpG), and particularly Article 25 and 25a for the land based casinos that specifically address AML/CFT points. The following transactions can take place in land based casinos: transactions in foreign exchange, purchases of chips in cash or credit card, payout of winnings in cash, cheque or transfer. No accounts are open. Electronic lotteries are included into the monopoly on games on chance by Article 12a GSpG and their regulation is based on Article 16(7) that mentions the obligation of issuing gaming conditions. Gaming Conditions are set out in administrative rulings of the MoF. The rulings have direct legal effect and must be respected by the licensee. Without the permission of the MoF gaming is not allowed. Breaches of gaming conditions are sanctioned by Article 14, paragraph 6 and Article 52 GSpG.

##### **Real Estate Agents, Dealers, Management Consultants and Insurance Intermediaries**

767. Pursuant Article 365m (1) GewO, measures to prevent ML and FT applies to natural and legal persons as well as legal entities and registered partnerships operating as dealers, real estate agents and management consultants. In Austria, a real estate agent is a physical person whose business is to negotiate the sale of real estate, parts of real estate, buildings on property belonging to other persons, site-leasehold interests, ownership of apartments, ground leases or floor-space tenancies.

768. Concerning dealers, including auctioneers, the GewO applies only to the extent that payments are made in cash in an amount of EUR 15,000 or more, no matter whether the transaction is executed in a single operation or in several operations which are linked or appear to be linked. The GewO also applies to the category of management consultants including organization development experts when performing the following services for companies or trusts:

- forming companies or other legal persons;
- acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

- acting as or arranging for another person to act as a trustee of a trust or a similar legal arrangement; or
- acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with EU legislation or subject to equivalent international standards.

769. As mentioned above, the authorities choose to designate the profession of management consultants as an Austrian equivalent for the FATF category of TCSPs. It appears that most of the activities that were previously performed by the management consultants were different than those listed above. Some of the above listed activities were not permitted to be performed by management consultants. On the other hand, at the time of the on-site visit, other professions were performing activities that enter the scope of TCSPs, such as office services providers, but in apparent contradiction with the new provisions of the GewO. The authorities explained that the chamber of commerce has to change the business profiles of these professions, in order to clarify that only management consultants are now authorized to perform TCSPs activities.

### **Lawyers**

770. For lawyers, the AML/CFT requirements and measures are governed by the Lawyer's Act, RAO, and the Disciplinary Statute for lawyers and lawyer-candidates (*Disziplinarstatut, DSt*, Federal Law Gazette Nr. 474/1990). The RAO includes in particular in its Article 8a-8f, 9, 9a and 12 AML/CFT requirements and measures. Besides, there are statutory regulations set down in the Directives of the Austrian Bar Association, in the first place the Directive on the practice of the lawyers' profession and the supervision of the lawyers' duties (*Richtlinien für die Ausübung des Rechtsanwaltsberufs und für die Überwachung der Pflichten des Rechtsanwaltes – RL-BA 1977*).

### **Civil Law Notaries**

771. The AML/CFT requirements for Notaries are mainly governed by the Notary's Act, NO, that includes AML/CFT requirements and measures, particularly in its Articles 36 to 37a. Other relevant documents are the Amendments to the Professional regulations 2008 (BRAG 2008) and the Notaries examination Act. In addition, the Austrian Chamber of Civil Law Notaries has issued Recommendations on the prevention of ML/FT, last updated in April 2008.

### **Chartered Public Accountants and Tax Consultants (*Wirtschaftstrehänder*)**

772. The relevant provisions are contained in the WT-ARL which is a regulation of the Chamber of chartered public accountants and tax consultants on the basis of Article 83, paragraph 2 of the WTBG. This Directive in its current version came into effect on May 1, 2008 and the relevant AML/CFT requirements are contained in Articles 34 to 38 WT-ARL.

### **Accountancy Professions**

773. The relevant provisions are contained in the BiBu-ARL, established by the Parity Commission for the Accountancy Professions and based on Article 69, paragraph 2 BiBuG. This Directive has the status of a regulation and its current version came into effect on April 23, 2008. The relevant AML/CFT requirements are contained in Articles 17 to 21 BiBu-ARL.

***CDD Measures for DNFBPs in Set Circumstances (Applying c. 5.1-5.18 in R. 5 to DNFBP) (c. 12.1)***

**Land-Based Casinos**

774. Casinos are not permitted to keep anonymous player accounts or accounts in fictitious names (c.5.1).

775. They are required to undertake CDD measures at the casino entrance irrespective of whether the customer will engage in financial transactions (Article 25, paragraph 1 GSpG). The CDD measures have to be undertaken when a foreign exchange of more than EUR 15,000 is performed in the casino. The CDD requirements in the case of foreign currency exchange are the same as the one referred to in Section 3 for banks. Indeed, the operations are realized by staff of the casino but on behalf of one of the commercial banks which has a contract with CASAG. The staff of the casinos is obliged to follow-up the CDD requirements of the BWG. Based on the “Safety measures to prevent money laundering” internally issued by the licensee, CASAG, and agreed by the MoF, “those persons who appear to have above average turnover will be monitored when they exchange cash for chips or cash their chips.” According to CASAG and the MoF, it is generally considered that the monitoring threshold is around EUR 700, which is the minimum income level mentioned in the GSpG, and is mandatory in the case of Austrian, EU and EEA citizens. According to the internal rules, a confirmation of winning is only issued in the head office of licensees after checking the correctness of stakes/winnings of the guest. These details have to be confirmed by executives of the casinos. A winning confirmation is drawn only on the recorded name of the guest. Winnings are paid out in cash or on special request by crossed cheque. The amount of the crossed cheque is only transferable to a registered bank account (opening of a bank account is subject to the AML/CFT-regulations contained in the BWG). A drawing of a crossed cheque is monitored by the licensee. According to CASAG, less than 10 certificates of winnings or crossed checks are issued on a yearly average. This said there is no legal requirement to identify transactions equal or above EUR 3,000 performed by non-EEA citizens (c.5.2).

776. Pursuant to Article 40(1) BWG, the identification and verification requirement at the entrance of the casino consists in the presentation of an official identification document with photo which complies with the requirements stated in Article 40(1) BWG (c.5.3). No customers are legal persons or arrangements (c.5.4) and the nature of the business relationships is clear in the case of a casino customer (c.5.6).

777. If there is a suspicion or a legitimate reason to assume that the customer does not act for his/her own account, the licensee has to ask the visitor to give proof of the beneficiary with the means described in Article 40(2) BWG (c.5.5).

778. As mentioned above, there is an ongoing monitoring of the business relationship when the transactions exceed an average of EUR 700. This appears to be a comprehensive monitoring, mostly based on the rules related to the promotion of responsible gambling that are foreseen in Article 25 (3) GSpG and apply to all EU/EEA citizens. According to the MoF and CASAG, the practice is to apply this regulation to every customer. No specific review is undertaken for other higher risk categories (c.5.7), as well as no enhanced due diligence for higher risk categories of customers, such as

nonresident customers (c.5.8). The possibility offered by the standard to the authorities to apply reduced or simplified CDD measures is not implemented in the Gaming act (c. 5.9-c.5.12).

779. The verification of the identity of the customer and beneficial owner is performed before the transaction, at the entrance of the casino or when transactions exceed EUR 700 (c.5.13-c.5.14).

780. When the customer does not comply with the CDD requirements, including at the entrance, the customer is not allowed to stay in the casino and the licensee has to inform the MoI (Article 25 (7) GSpG). It has to be noted that this later obligation is broader than the standard (c.5.15).

781. Where the customer is already in the casino and refuses to comply with CDD requirements when performing a transaction above the EUR 700 threshold, ultimately “the casino management shall question the player on his/her income and assets, and depending on the information obtained in this way, shall warn him/her and ban him/her if necessary” (Article 25 (3) GSpG). It has also to be mentioned that the management of the gaming establishment may deny entry to any person without stating reasons pursuant to Article 25 (2) GSpG (c.5.16). A customer is identified each time he/she enters or re-enters a casino in Austria (c.5.17).

782. The new amendments to the GSpG, including enhanced identification measures and inclusion of terrorist financing, were only enacted in July 2008 and were consequently too recent to be assessed for their effective implementation. But the pre-existing requirements appear effectively implemented by the 12 licensees, mainly because they share common patterns with the requirements related to the promotion of responsible gaming and are supported by the recently appointed compliance officer and by the work of the internal audit department.

### **Internet Casinos (Electronic Lotteries)**

783. Upon the Austrian legislation, and Article 56 (1), it is forbidden to provide the means to receive winnings from foreign games of chance within Austria or allowing winnings to be received in any other way. The MoF is confronted with foreign based internet gambling and has already made several indictments for breaches of the license requirement in gambling law. These foreign based internet gambling providers are subject to the foreign supervision of their host state. Several (sanctions) procedures are pending. Up to now there is no proof of foreign internet providers being managed from Austria.

784. There is only one company in Austria authorized by the GSpG to conduct lottery business, and this includes electronic lotteries ([www.win2day.at](http://www.win2day.at)). According to Article 16 (1) GSpG, the licensee must provide conditions of entry for the games of chance for which it has a license. These are subject to the prior approval of the Federal Minister of Finance. Pursuant to Article 16 (7), the gaming conditions for electronic lotteries should include at a minimum the regulation of:

- the amount of the lottery player’s stake and any administrative costs which may have to be paid;
- the relationship which the winning sum bears to the amount of the stake; and
- how winnings are to be claimed and paid out.

785. The Gaming conditions for Electronic lotteries are in effect since October 31, 2006. Some of their provisions address the CDD issues. There is a general obligation to register, to communicate ID (name, address and date of birth) as well as the details of an Austrian bank account (Article 3.1. of the gaming conditions) and identity details are compared with entries in official registries, administered by the authorities. It should be noted that players may only use EUR 800 per week to take part in Electronic Lotteries (Article 3.7 of the Gaming conditions). The licensee applies a constant risk-based monitoring on the ongoing transactions, mostly in its functions of ensuring responsible gaming.

786. Nevertheless, the requirements set up by the standard do not apply to payments made to the electronic account in order to initiate a game. But the need for CDD exists when winnings are paid out as they can exceed EUR 3,000. The practice is to pay the winnings on the bank account that was declared by the customer at the beginning of the business relationship.

787. It was understood by the assessors that the licensee has no power to check that the bank account declared is really the one of the customer, nor to verify the identity of the customer. Database checks are made but they will only prove the existence of one person, but will not enable to ascertain that there is no identity theft. In the case of a payment of winnings exceeding EUR 3,000, there are no requirements to apply the recommendations detailed in criteria 5.1 to 5.18, except for the prohibition of fictitious accounts (c.5.1), identification of the customer (c.5.2) and prohibition of customers that are legal persons (c.5.4, c.5.5.2).

788. According to the information received by the assessor, the gaming conditions appear effectively implemented. Even if there are no ML/FT specific requirements, the obligation to ensure responsible gaming covers CDD related issues and appears consistently implemented by the single licensee. A dedicated fraud team permanently monitors all transactions and all accounts with pay-in of more than EUR 400 per week receive additional scrutiny. Those accounts represent less than 2 percent of the total number of accounts.

### **Real Estate Agents, Dealers, and Management Consultants**

789. Due to the specificities of their activities, designated trade and business persons are not permitted to keep anonymous accounts or accounts in fictitious names (c.5.1).

790. According to Article 365o GewO, they are required to undertake CDD measures when:

- establishing a business relationship;
- carrying out occasional transactions amounting to EUR 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- there are doubts about previously obtained customer identification data.

791. Consequently, a EUR 15,000 threshold applies to the CDD requirement of real estate agents and management consultants (c.5.2).

792. Customer due diligence measures comprise identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source (Article 365p(1)1 GewO). A definition is contained in the explanatory notes to the Trade Act (GewO) which are part of the legislative proposal sent to the parliament. According to these explanatory notes, an official photo identification means a document edited by an authority, containing a picture and a signature. The definition relates to Article 40, paragraph 1 BWG. According to the principle of the unity of the law, this definition is valid also for the Trade Act. It has to be noted that pursuant to Article 365p(2), the extent of the CDD requirements set out in Article 365p(1) GewO shall be determined by the actual risk profile depending on the type of customer, business relationship, product or transaction. This is confirmed in the explanatory note to the GewO, which states that “the system is a flexible one” (c.5.3). Concerning real estate agents, the law does not precise if they should comply with CDD requirements with respect to both the purchasers and the vendors of the property. But, regarding Article 365y on record keeping, the explanatory note to the GewO indicates that “real estate agents have to keep copies of the documents of both the intermediated customers...”

793. For customers that are legal persons or legal arrangements, the GewO does not contain specific requirements to verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person. But reference to requirement to identify and to verify the legal status of the legal person or legal arrangement is made in the explanatory note to the GewO (c.5.4).

794. The designated tradespersons are required to “identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that it is satisfactorily known who the beneficial owner is. As regard legal persons, trusts and similar legal arrangements, this includes taking risk-based and adequate measures to understand the ownership and control structure of the customer” (Article 365p(1)2 GewO). It has to be noted that the GewO subjects the CDD concerning the beneficial owner on a risk-base. The explanatory notes to the trade act give general guidance to the designated persons in order to help them identify the risks that are foreseen in Article 365p(1)2 GewO. But no specific guidance has been given concerning what is foreseen as a risk-based identification and verification of the beneficial owner. There is no mention in the law on the need to take reasonable measures in order to determine who are the natural persons that ultimately own or control the customer (c.5.5).

795. Pursuant to Article 365p(2) GewO, the designated tradespersons are required to obtain information on the purpose and intended nature of the business relationship (c.5.6).

796. They are also required to conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the entity's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date (Article 365p(1)4 GewO). The law and its explanatory notes do not contain any precisions on the means to keep the information up-to-date and relevant, particularly in relation with higher risk categories of customers or business relationships (c.5.7).

797. Except for PEPs and non-face-to-face transactions, the designated tradespersons are not required to perform enhanced due diligence for higher risk categories of customers, business relationships or transactions (c.5.8).

798. In addition to the general risk based approach adopted by the law for CDD (Article 365p(2) GewO), simplified CDD procedures are mentioned in Article 365r(1) GewO. It has to be mentioned that in the listed cases, there is no need for CDD at all. Those cases are the same as the one listed in Article 40a(1)BWG and the relevant analysis can be found under section 3. Other exemptions of the CDD requirements are mentioned in Article 365r(2) GewO that are in relation with low risk insurance products, in line with the examples given by the FATF, as well as electronic money transactions of low value with the same restrictions mentioned in Article 40a(3)1 BWG (c.5.9).

799. In the above mentioned cases, the exemption of CDD is valid, under conditions, for customers resident in all the EU countries and also third countries. No detailed guidance has been given on the list of countries that the Austrian authorities consider in compliance with and having effectively implemented the FATF recommendations. According to the authorities, the European Commission is the competent authority to list countries that are not under laws equivalent to the provisions of the Third EU ML Directive. The explanatory note give general explanation to the last amendment to the trade act that transposed the Third EU ML Directive, but no specific guidance is available for the designated tradespersons in order to determine precisely the customers that are exempted from the CDD obligation (c.5.10).

800. Pursuant to Article 365o1 GewO, the obligation to perform CDD applies regardless of any derogation or exemption when there is a suspicion of ML or FT. But, pursuant to Article 365r(1), Article 365p(2), which refers to risk profile, should not apply in case of simplified CDD procedures. Consequently, there is no obligation to perform CDD measures when specific risk scenarios apply (c.5.11).

801. No specific guidelines have been issued by the competent authority regarding the extent of the CDD measures on a risk sensitive basis. The WKO is the relevant institution for the information of tradespersons (c.5.12).

802. Pursuant to Article 365q(1), the designated trade persons have to verify the identity of a customer and beneficial owner before establishing business relationship or carrying out of a transaction. Real estate transactions carried out by a real estate agent should require verification of identity if the annual rent amounts to EUR 15.000 or more (c.5.13).

803. If the amount is unknown at the beginning of the transaction, the trade or business person should verify the identity as soon as the amount is known or can be ascertained and it becomes obvious that this threshold will be reached or exceeded (Article 365q(1)). By way of derogation from the obligation to identify before establishing business relationship or carrying out of a transaction, verification of the identity of the customer and the beneficial owner may be completed during the establishment of a business relationship where it is necessary not to interrupt the normal conduct of business and risk of money laundering or terrorist financing is limited. In such situations, these verification procedures should be completed as soon as possible after the initial contact. It has to be noted that the designated tradespersons are currently not required to adopt risk management

procedures concerning the conditions under which the utilization of the business relationship prior to verification may occur (c.5.14).

804. Pursuant to Article 365p(4), whenever trade or business persons are unable to comply with CDD requirements, they should be obliged to refrain from conducting transactions through a bank account, from establishing any business relationship, from carrying out the transaction, or to terminate the business relationship. Moreover, they should examine the necessity of making a suspicious transaction report to the MoI (c.5.15).

805. Pursuant to Article 365q(2), where tradespersons have already commenced the business relationship, they have to complete CDD “as soon as practicable.” No guidance has been issued to the tradespersons in order to determine at which point they should consider that they are unable to comply and follow the requirements mentioned in Article 365p(4) (c.5.16).

806. Pursuant to Article 365p(3), the CDD obligations have to be met in respect of customers already existing (c.5.17-18).

807. According to interviews the assessors had with non-financial businesses and professions subject to the GewO, the implementation of CDD requirements appeared to be generally superficial. This is related to a relatively recent legal framework, the small size of most of the businesses that already have to implement a number of regulations and lack resources, the general idea that the risks are low, and the limited extent of AML/CFT supervision.

### **Lawyers and Notaries**

808. The legal requirements on CDD are the same for lawyers and notaries and will be addressed jointly. The only difference is the existence of guidelines issued by the Chamber of Notaries. These guidelines are not binding but may usefully inform on the professional organization’s reading of the law.

809. The RAO and the NO do not allow lawyers and notaries to keep accounts other than escrow accounts to pay third party money, and consequently are not allowed to keep anonymous accounts or accounts in obviously fictitious names. The escrow bank accounts are regulated by the BWG and respectively the RAO for lawyers and NO for Notaries. In addition, these accounts are subject to the supervision of the professional organizations (c.5.1).

810. Pursuant to Article 8a (1) RAO and Article 36a(1) NO, the following activities of lawyers and notaries can be subject to the CDD requirements when they prepare for or carry out transactions for a client in relation to them:

- buying or selling of real property or business entities;
- management of client monies, securities or other assets, the opening or management of deposit, savings or securities accounts; and
- creation, operation or management of trust companies, business entities or similar structures such as trusts or foundations, including the procurement of the funds required for the creation, operation or management of companies.

811. It has to be mentioned that scope of the CDD requirements is unclear from the reading of the first paragraph of Article 8a (1) RAO and Article 36a(1). Indeed, it requires lawyers and notaries to “examine especially carefully all operations, which, due to their nature, could apparently be in connection with money laundering (Article 165 StGB) or terrorism financing (Article 278d StGB), and for which he realizes a financial or real estate transaction in name or on the account of his party or in the planning or realization of which he participates for his party” concerning the above listed activities. This introduces a possible confusion that a double condition is required in order to perform CDD obligations, including the apparent connection with ML or FT. This possible confusion has been acknowledged by the Chamber of notaries clarifying in its guidelines that the above listed activities are transactions susceptible of money laundering and, as such, the CDD requirements have to apply. Guideline of the Chamber of notaries is not binding. There are currently no guidelines for lawyers, but the Bar Association view is that the CDD requirements apply to all listed activities, whenever there is or not an apparent connection to ML or FT. Nevertheless, MoJ considers to suggest a clarifying amendment of Article 8a(1) RAO and Article 36a(1) NO to the Austrian parliament as soon as possible.

812. Pursuant to Article 8b(1) RAO and Article 36b(1) NO, and in the cases listed in Article 8a(1) RAO and Article 36a(1) NO, lawyers and notaries have to undertake customer due diligence (CDD) measures, including identifying and verifying the customer’s identity (Article 8b, paragraph 1 RAO), when:

- establishing a business relationship on a continuing basis before the acceptance of the mandate; or
- concerning all other transactions which amount to an order sum (total contract value assessed according to the Lawyer’s Fees Act respectively the Notarial Tariff Act) of at least EUR 15,000 regardless whether the transaction is realized in one single action or in several actions which seem to be connected, prior to the realization of such transaction. If the order sum is at first unknown, the identity has to be established as soon as it is foreseeable or determined that the expected order sum will exceed an amount of EUR 15,000; or
- they know, suspect or have legitimate reason to assume that the operation serves for the purpose of ML or FT; or
- there are doubts about the veracity or adequacy of previously obtained customer identification data.

813. It has to be noted that the requirements appear more restrictive than the standard regarding the business relationship, with the undefined mention of “continuing basis” in the first bullet (c.5.2).

814. According to Article 8b(2) RAO and 36b(2) NO, lawyers and notaries have to identify the client and verify the client's identity on the basis of documents, data or information obtained from a reliable and independent source. Guidelines for Notaries (section 8) stipulate that passports or personal IDs are suitable documents to prove a person’s citizenship (c.5.3).

815. The same provisions apply for legal persons and legal arrangements, requiring to verify that any person purporting to act on behalf of the customer is so authorized, and to identify and verify the identity of that person. The guidelines for notaries indicate how to identify and verify the legal status of the legal person or arrangement (c.5.4).

816. According to Article 8b(4) RAO and 36b(4) NO, the lawyer or the notary has to establish and verify the identity of the beneficial owner taking risk-based and adequate measures. Article 8d RAO and Article 36d NO define the notion of beneficial owner, as including:

in the case of corporate entities:

- the natural persons who ultimately own or control a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Community Law or subject to equivalent international standards; a percentage of 25 percent plus one share should be deemed sufficient to meet this criterion;
  - the natural persons who otherwise exercise control over the management of a legal entity;
- in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
- where the future beneficiaries have already been determined, the natural persons who are the beneficiary of 25 percent or more of the property of a legal arrangement or entity;
  - where the individuals that benefit from the legal arrangement or entity have yet to be determined, the group of persons in whose main interest the legal arrangement or entity is set up or operates; and
  - the natural persons who exercise control over 25 percent or more of the property of a legal arrangement or entity.

817. It has to be noted that there is no automatic obligation to identify and verify the beneficial owner, as the lawyers and notaries have to rely on a risk-based approach (c.5.5).

818. According to Article 8b(6) RAO and Article 36b(6) NO, the lawyer or the notary has to gather information on the purpose and intended nature of the business relationship (c.5.6).

819. Pursuant to the same article, lawyers and notaries have to conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the client, the business and risk profile, including, where necessary, the source of funds. They have to ensure that the documents, data or information held are kept up-to-date. It has to be noted that there is no requirement to ensure that the documentation is relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships (c.5.7).

820. There is no requirements to perform enhanced due diligence for higher risk categories of customer, business relationships or transactions, other than for the specific risks assessed under R.6 and R.8 (c.5.8).

821. Lawyers and notaries are allowed to have simplified due diligence procedures in the cases listed in Article 8e(1) RAO and Article 36e(1) NO. These are the same cases that are contained in Article 40a(1) and (2) BWG, and relevant analysis concerning the extent of these cases and guidelines

that are necessary can be found in section 3. In addition, the RAO and NO include cases that are not listed in the BWG. Pursuant to Article 8e(1)6 RAO and Article 36e(1)6, simplified CDD applies for any legal person:

- a) which resides in a Member State which has subjected its activities to the provisions of Article 4 of Directive 2005/60/EC, and which is subject to supervision by the competent authorities according to Article 37, paragraph 3 of the Directive, with non-compliance with the requirements of the Directive entailing effective, proportionate and deterrent sanctions;
- b) whose identity can be publicly verified, is transparent and established beyond doubt;
- c) which requires, before undertaking financial activities, mandatory authorization under national law that may be denied for lack of trustworthiness and expertise of the natural person or beneficial owner managing the business, and which is subject to comprehensive monitoring (including in-depth on-site examinations) by the competent authorities.

822. It also applies to a business establishment of a person mentioned above, if and to the extent that the Member State has subjected the activity of this establishment to the provisions of Directive 2005/60/EC.

823. It has to be noted that in the absence of guidance it appears difficult for a lawyer or a notary to ascertain that the exemption applies to the party, and to estimate what is considered by Article 8e(2) RAO and 36e(2) NO as “sufficient information to be able to reliably determine that the exemption applies” (c.5.9).

824. At the time of the on-site visit<sup>41</sup>, no guidance has been given by the authorities to lawyers and notaries in order to limit the scope of the exception to the CDD requirements to countries the authorities consider in compliance with and having effectively implemented the FATF Recommendations (c. 5.10).

825. Pursuant to the reference to Article 8b(1)3 in Article 8e(1) RAO, and 36b(1) 3 in Article 36e(1) NO, the exemption of CDD measures is not acceptable whenever there is a suspicion of money laundering or terrorism financing. It has to be noted that there is no reference to the requirement to perform CDD if specific higher risk scenario apply (c.5.11).

826. The Austrian Bar is currently preparing guidance that will include assistance to its members to determine the extent of the CDD measures on a risk sensitive basis. The information given in the guidelines issued by the Chamber of Notaries on this subject is limited. (c.5.12).

---

<sup>41</sup>In the meantime, such guidance has been given by the Austrian Bar to the lawyers. The lists of countries have been published via Infomail, which is sent via e-mail to the Austrian lawyers, and via the Austrian Lawyers’ Journal (“*Österreichisches Anwaltsblatt*”). The Chamber of Civil Law Notaries has informed their members in two newsletters about third countries which are currently considered as having equivalent AML/CFT systems to the EU on the one hand and risk countries on the other hand (November 2008, January 2009). The January 2009 version of the AML/CFT guidance contains information on this subject.

827. Pursuant to 8b(1) RAO, and 36b(1) NO, the lawyer or notary is required to verify the identity of the customer and beneficial owner before establishing a business relationship or conducting a transaction for occasional customers (c.5.13 and c.15.14).

828. Where the lawyer or the notary is unable to comply with the CDD requirements, no instruction can be accepted and the transaction should not be carried out. Business relationships already started should be discontinued. Moreover, a notification to the BKA has to be considered. The reporting to the BKA is mandatory if the party did not comply voluntarily with the requirement of disclosing its identity. It has to be noted that these requirements do not apply if the lawyer or the notary is providing legal advice or when representing the party in court or before a subordinate authority or public prosecution office, unless it is evident that the party was seeking legal advice solely for the purpose of ML or FT (c.5.15 and c.5.16).

829. There is no requirement to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times (c.5.17).

830. It is difficult to precisely assess the effective implementation of CDD measures by notaries and lawyers across the regions of Austria. But a high level of awareness was remarked from meeting with SROs and professionals, especially notaries. The fact that AML/CFT issues are incorporated in routine supervisory missions, and that sanctions have already been pronounced based on non compliance of AML/CFT requirements seems to be a factor of this awareness, as well as the guidance work done by the SRO in the case of notaries.

### **Chartered Public Accountants, Tax Consultants and Accountancy Professions**

831. Accountants may not keep anonymous accounts or accounts in obviously fictitious names as the opening of accounts by accountants is not foreseen by the professional regulations or the BWG (c.5.1).

832. Pursuant to Article 33 (1) WT-ARL and Article 16(1) BiBu-ARL, CDD requirements have to apply when:

- establishing a business relationship;
- carrying out occasional transactions amounting to EUR 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- there is a suspicion of ML/FT; and
- there are doubts about the veracity or adequacy of previously obtained customer identification data.

833. It has to be noted that the preparation of the above mentioned activities is not subject to CDD requirements. In addition, according to Article 33(2) WT-ARL and Article 16(2) BiBu-ARL, the establishment of a business relationship can only be assumed if a free consultation is followed by further services and orders, and if a certain duration is envisaged at the beginning of the business relationship. Consequently, activities like the creation of a company if the accountants' fees are under

EUR 15,000 are not subject to CDD requirements. The drafting of Article 34(1),(2) and (3) WT-ARL seems to narrow the scope of the CDD:

- “(1) Persons entitled to practice said professions shall be obligated to subject to particularly close scrutiny any service that specifically suggest a connection with money laundering.
- (2) Such particularly close scrutiny shall comprise the verification of all relevant circumstances, in particular with respect to customer’s identity, the actual content of the order and the customer’s will.
- (3) Due diligence measures shall comprise:....”Consequently it is possible to understand that CDD requirements will only have to be performed when a service specifically suggest a connection with ML. It has to be mentioned that there is no requirement of CDD in relation to FT. Dealing with CDD measures in a specific Article 17(1), the BiBu-ARL does not lead to the same ambiguities. In addition, according to Article 34(5) WT-ARL and Article 17(3) BiBu-ARL, the extent of due diligence measures required have to be determined on a basis commensurate to the overall risk of the business relationship (c.5.2).

834. Pursuant to Article 34(3)1 WT-ARL and Article 17(1)1 BiBu-ARL, accountants are required to identify and verify customers’ identity on the basis of documents, data or information obtained from a reliable and independent source, such as a valid official photo identity card (c.5.3).

835. If the customer is a legal person or a legal arrangement, their legal status has to be verified by obtaining a company register extract (Article 34(3)3 WT-ARL and Article 17(1)3 BiBu-ARL). The accountant is also required to verify that a person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person (c.5.4).

836. If the customer does not act on its own behalf, the identifying duty should also apply to the beneficial owner (Article 34(3)2, 34(3)3 WT-ARL and Article 17(1)2, 17(1)3 BiBu-ARL). Concerning legal persons, the notion of beneficial owner is defined in Article 34(4) WT-ARL and Article 17(2) BiBu-ARL. The definition is in the scope of the FATF glossary, but it is limited to natural persons holding more than 25 percent of direct or indirect ownership or control. This could prevent the ability to ascertain the natural persons that ultimately own or control the customer. The identity of the beneficial owner has to be verified by mean of appropriate measures. It has to be noted that those measures have to be taken in accordance with the overall discernible risk of the business relationship. No specific guidance on risk has been given to accountants. In addition, there is no requirement to understand the ownership and control structure of the customer (c.5.5.).

837. Pursuant to Article 34(3)5 WT-ARL and Article 17(1)5 BiBu-ARL, accountants are required to obtain information on the purpose and intended nature of the business relationship (c.5.6).

838. Accountants are also required to take measures to ensure that the risk profile of the business relationship is up to date (Article 34(3)6 WT-ARL and Article 17(1)6 BiBu-ARL). It has to be noted that there is no other mention of any requirement of ongoing due diligence in the WT-ARL, or any guidance given to the accountants (c.5.7).

839. The requirement of enhanced due diligence for higher risk business relationships mentioned in Article 37(1) WT-ARL and Article 20(1) BiBu-ARL should be applied in all cases which represent a higher ML/FT risk but is only specified for non-face-to-face transactions and PEPs. There is no guidance to assist accountants to determine what the other higher risks are (c.5.8).

840. Low risk situations are determined under Article 36 WT-ARL and Article 19 BiBu-ARL. These are the same situations mentioned in the BWG. It should be mentioned that there is a total exemption of CDD measures in these cases, provided that there is sufficient information to determine whether a person is eligible (c.5.9).

841. This exemption of CDD can be applied to customers resident in another country of the European Union as well as to customers resident in third countries. The Austrian authorities did not indicate which countries they consider to be in compliance with and have effectively implemented the FATF Recommendations (c. 5.10).

842. Pursuant to Article 36 WT-ARL and Article 19 BiBu-ARL, simplified CDD measures are not acceptable whenever there is suspicion of ML or FT. (c.5.11).

843. No guidelines have been issued by the Austrian authorities concerning the extent of the CDD measures that can be determined on a risk sensitive basis (c.5.12).

844. Pursuant to Article 34(6) WT-ARL and Article 17(4) BiBu-ARL, the identity of the customer has to be established and verified before the establishment of a business relationship or the performance of a transaction. In situations where it is necessary to avoid interrupting the normal business procedures and the risk of ML or FT is low, this may be completed during the establishment of the business relationship. In this case, the relevant procedures have to be completed as soon as possible after the first contact. It has to be noted that accountants are not required to adopt risk management procedures concerning the conditions under which this may occur (c. 5.13 and c.5.14).

845. Pursuant to Article 35(1) WT-ARL and Article 18(1) BiBu-ARL, when the accountant is unable to comply with CDD, it is prohibited to establish a business relationship or to conduct a transaction. In such cases, existing business relationships have to be terminated. In addition, accountants have to consider making a STR. It has to be noted that these requirements do not apply within the framework of an assessment of the customer's legal position or within the framework of a function as the customer's defense counsel or representative in or in connection with a court proceeding, including counseling about the institution or avoidance of an action, as accountants in Austria are involved in tax proceedings (c.5.15 and c.5.16).

846. Accountants have to apply CDD requirements to existing business relationships, on a risk-oriented basis, before December 31, 2008 (Article 34(7) WT-ARL and Article 17(5) BiBu-ARL. It has to be noted that this requirement does not clearly extend to the obligation to identify the beneficial owner when a customer does not act on its behalf (c.5.17).

847. From the meeting held with the authorities and the professionals, the level of implementation of CDD measures by accountants does not appear particularly important. This impression is related to the absence of effective AML/CFT supervision of this profession, the important number of accountants, a shared view by professionals and their SROs that the risk of ML/FT is low in Austria,

that other professions than accountants are more at risk, and that it is still difficult to obtain information from the clients.

***CDD Measures for DNFBPs in Set Circumstances (Applying Criteria under R. 6 & 8-11 to DNFBP) (c.12.2)***

**Land Casinos**

848. Concerning Recommendation 6, there is no legal or regulatory requirement to put in place appropriate management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person. It is worth noted that approximately two thirds of the total betting volume is related to foreign nationals, when they only count for approximately one third of the customers.

849. Concerning Recommendation 8, there are no legal or regulatory requirements to have policies in place or to take measures to prevent the misuse of technological developments in ML or FT schemes. But land based casino in Austria are not concerned by this issues, to the exception of payments by credit cards which are specifically monitored according to the internal “Safety measures to prevent money laundering”, section 2.3.3. In addition, the land-based casino does not provide for non-face-to-face transactions. Specific internal procedures, similar to the one applying to certificate of winnings or crossed cheques, apply when a client requests the funds to be transferred to a bank account.

850. Recommendation 9 is not applicable in the case of Austrian land-based casinos.

851. Concerning Recommendation 10, casinos are required to maintain information on the visitors identified at the entrance for at least five years (Article 25 (1) GSpG). It is the only information they are legally required to keep. According to the internal guidelines approved by the MoF, any purchasing or cashing transaction above around EUR 700 is recorded and allocated to the client’s name, unless the client’s identity has already been recorded and allocated to the client’s name (e.g., payments by traveler cheques and credit cards). The payment of winnings in form of chips to guests at the gaming tables is recorded in the same way and allocated to the guest’s name. All records are transferred from all casinos to the headquarters in Vienna on a daily basis. There is no information on the period these records are maintained but according to the MoF and CASAG, the five years requirement is met. Pursuant Article 51 GSpG, game secrecy applies concerning the players and their participation in the game. There is an exception to the game secrecy in the case of Article 25 (6) and (7) GSpG. Article 25(6) mentions the application of Article 41 (1) penultimate sentence, (3),(4) and (7)BWG to the licensee, but this does not include Article 41(2) which requires providing the Federal Ministry of Interior with all information which it deems necessary in order to prevent or pursue cases of ML or FT. Accordingly, the gaming secrecy prevents the casinos to ensure that all customer and transaction records and information are available to domestic competent authorities unless a court order is issued. In this case the game secrecy is lifted (Article 51(2) GSpG).

852. Concerning Recommendation 11, Article 25(6) GSpG mentions the application of Article 41(1) penultimate sentence, which requires casinos to “pay special attention to any activity which they regard as particularly likely, by its nature, to be related to ML or FT, in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent

economic or visible purpose” but there is no mention of the duration of the record-keeping requirement. In addition, CASAG internal guidelines against ML provide for special attention in the case of the payout of winnings in cash, by cheque or transfer to a bank account (section 2.3.3).

### **Internet Casinos**

853. Concerning Recommendation 6, there is no legal or regulatory requirement to put in place appropriate management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person. It has to be mentioned that only Austrian residents are allowed to play on [www.win2day.at](http://www.win2day.at), which limits the possibility of a customer being a foreign PEP, to some extent.

854. Concerning Recommendation 8, the licensee operating the Internet casino is aware of the risk related to the misuse of technological developments in ML or FT schemes. This is the reason why the gaming conditions request for the provision of both an identification document and an Austrian bank account. But as it has been shown before, the checks that are performed do not enable to verify that the customer is not using a fake identity and that its bank account matches the given identity. But the authorities consider that the risk of this specific misuse is very low.

855. Recommendation 9 is not applicable, as the relation is directly between the customer and the casino.

856. The Licensee maintains records of all transactions. But there is no legal obligation to this effect (R.10). In addition, there is no requirement to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose (R.11).

### **Real estate agents, dealers, management consultants and insurance intermediaries**

857. Concerning Recommendation 6 and pursuant to 365s (3) GewO, the designated tradespersons must:

- have appropriate risk-based procedures to determine whether the customer is a politically exposed person (PEP), also if holding a domestic public function;
- have senior management approval for establishing business relationships with such customers;
- take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction and
- conduct enhanced ongoing monitoring of the business relationship.

858. It has to be mentioned that this Article, or Article 365n(4) which defines PEPs, do not require enhanced due diligence for PEPs that are only potential customers. The definition of PEPs does not mention important political party officials. In addition, if the senior management approval is required for establishing a business relationship with a PEP, there are no provisions for cases where a customer subsequently becomes a PEP. The obligation to establish the source of wealth and source of funds is limited to that involved in the business relationship or transaction.

859. Concerning Recommendation 8, and according to Article 365s, paragraph 5 GewO, tradespersons have to pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favor anonymity, and take measures, if needed, to prevent abuse. The main examples are non-face-to-face business activities. In case of distance transactions, tradespersons have to send order forms to the customer's residence by means of registered mail. The customer must return the order form with the addition of a readable copy of an official photo identification, with which the tradesperson has to verify the data of identity in the order form (Article 365s(1)). Enhanced due diligence also applies in the case of on-line auctions (Article 365s(2)).

860. The GewO does not allow the designated trade persons to rely on intermediaries or other third parties to perform the CDD requirements (R.9).

861. Concerning Recommendation 10, and pursuant to Article 365y(1) GewO, the designated tradespersons are required to maintain records regarding the verification of identity and any supporting evidence and records concerning business relationships and transactions. The records have to be kept for at least five years after carrying out the transaction or after ending the business relationships. In case of liquidation of the company, the records are kept for seven years by the liquidator. The records have to be available to the MoI or other competent authorities in case of possible ML or FT. In general, the Austrian police did not encounter problem of access to data during its investigations.

862. Regarding Recommendation 11 and pursuant to Article 365t GewO, tradespersons have to pay special attention to any activity which they regard as particularly likely to be related to ML or FT, in particular complex or unusually large transactions or all unusual patterns of transactions which have no apparent economic or visible lawful purpose. It has to be noted that there is no requirement to set forth the findings of the examination of these transactions in writing.

### **Lawyers and Civil Law Notaries**

863. Pursuant to Article 8f(1) RAO and Article 36f(1) NO, lawyers and notaries are required, in addition to the performing the common CDD measures, to verify whether the party is a politically exposed person residing in another EU Member State or a third country. In order to be able to determine PEPs, they should apply adequate risk-based procedures. The definition of a PEP is given in Article 8f(2) RAO and Article 36f(2) NO, and includes a reference to the beneficial owner. It has to be noted that it does not include reference to important political parties' officials, and there is no mention of the case where a PEP is a potential customer. The Chamber of notaries gives guidance to its members on the measures that could form part of the risk management system to determine whether a potential client is a PEP. A sample questionnaire has been circulated to the profession, and every notary is allowed to contact the Notary Bank in order to have a free access to a commercial electronic database of PEPs. The Austrian Bar is currently preparing guidance that will cover the issue of PEPs. It also has to be noted that, as a consequence to the criteria of residence of the PEP, a foreign PEP residing in Austria will not be subject to the provisions of Article 8f(1) RAO and Article 36f(1) NO (c.6.1).

864. A mandate-relation with a PEP residing in another member state or a third country can only be established upon prior authorization of the lawyer (one of the lawyers authorized to manage the

lawyer company), according to Article 8f(3) RAO. Such obligation related to senior management approval does not exist in Article 36f(3) NO because the notarial profession can only be exercised by the notary himself who is personally appointed to officiate or by an (independent) substitute notary (Article 123 NO). In addition, there is no requirement regarding an accepted customer or a beneficial owner that is subsequently found to be, or becomes a PEP (c. 6.2).

865. In the case of foreign PEPs, the lawyer or the notary are required to take appropriate measures to check the origin of the funds which are being used for the business relationship or the transaction (Article 8f(3) RAO and Article 36f(3)NO). It has to be noted that these articles do not require establishing the source of wealth and the source of funds of customers, as they only address the framework of a business relationship or a transaction (c.6.3).

866. Pursuant to the same articles, lawyers and notaries are required to conduct enhanced ongoing monitoring of PEPs (c.6.4). The CDD requirements do not extend to domestic PEPs who reside in Austria, being limited by Article 8f(1) and Article 36f(1) to PEPs residing in other EU Member States or third states (additional c.6.5).

867. It is difficult to assess the effective implementation of the CDD requirements related to PEPs by lawyers and notaries. But the higher risk profile of this clientele seems to be recognized by the persons met by the assessors. In addition, the Recommendations issued by the Austrian Chamber of Civil law notaries include a comprehensive sample questionnaire for self-declaration of PEPs. Information on the CDD requirements related to PEPs has been published in the Austrian lawyers Journal and provided in seminars and training courses.

868. There are no general requirements to lawyers or notaries to have policies in place or take measures if needed, to prevent the misuse of technological developments in ML or FT schemes (c.8.1).

869. Pursuant to Article 8b(3) RAO and Article 36b(3) NO, if the party is not physically present when establishing the business relationship or conducting the transaction, lawyers and notaries are required to “take additional appropriate and conclusive measures to establish the identity of the party in a reliable way and to ensure that the first payment of the party in the framework of the operation is realized through an account opened in the name of the party at a credit institution to which Directive 2005/60/EC is applicable.” The explanatory notes to the amendment to the Professional Regulations 2008, on Article 8a RAO explain that each lawyer has to find the appropriate means for his/her own law firm. But no specific guidance has been issued to help lawyers and notaries determine what “additional appropriate and conclusive measures” should be in the context of non-face-to-face business. The requirement to apply these policies and procedures should apply on an ongoing basis based on Article 8a(2) RAO (c.8.2).

870. Lawyers and notaries are not permitted to rely on intermediaries or other third parties to perform any elements of the Customer Due Diligence process (c.9.1 to c.9.5).

871. Pursuant to Article 8b(5) RAO and Article 36b(5) NO, lawyers and notaries have to retain the documents submitted to establish the identity of the client and the beneficial owner, as originals if possible. With official photo identifications and other documents which cannot be retained as originals, or where this would be unsuitable, lawyers and notaries have to produce and retain

photocopies. Pursuant to Article 12(3) RAO and Article 49 (3) NO, there is a requirement to maintain records on all transactions referred to in Article 36a(1) RAO and 8a(1) NO, with the limitation already mentioned that those articles only clearly oblige to scrutinize all transactions whose nature suggests that they could be related to ML or FT (c.10.1).

872. There is a requirement to maintain records of identification data for at least five years following the termination of a relationship with a party. The same requirement prevails for the transactions referred to in Article 36a(1) RAO and 8a(1) NO. There is no mention on the requirement to keep records longer if requested by a competent authority in specific cases (c.10.2).

873. The same reference to a transaction set out in Article 36a(1) RAO and 8a(1) NO applies to the requirement that a lawyer or a notary has to provide upon request of the MoI (BKA) all information he or she is aware of to the extent required to clear a suspicion of ML or FT directed against a party (Article 37(4) RAO and 9(4) NO). It has to be noted that this obligation is waived if the party was seeking legal advice or when representing him/her in court or before a subordinate authority or public prosecution office, unless it is evident that the party was seeking legal advice solely for the purpose of ML or FT (c.10.3).

874. There is no specific obligation for notaries and lawyers to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose (c.11.1 to c.11.3).

### **Chartered Public Accountants, Tax Consultants and Accountancy Profession**

875. According to Article 37 (1)2 WT-ARL and Article 20 (2) BiBu-ARL, enhanced due diligence measures have to be conducted with respect to transactions or business relationships with PEPs, including the compliance with appropriate and risk-based procedures to determine whether the customer is a PEP. For the professions regulated by the WT-ARL, this enhanced CDD is nevertheless limited by the reference to Article 34(1) WT-ARL and the need to be in presence of a service that specifically suggests a connection with ML. The notion of PEP is defined in Article 37(1)3 WT-ARL and Article 20(3) BiBu-ARL. It has to be noted that it does not include reference to important political parties' officials, and there is no mention of the case a PEP is a potential customer. (c.6.1). In the case of accounting firms, there is no requirement to obtain senior management approval for establishing relationships with a PEP (c.6.2).

876. Pursuant to Article 37(1)2c WT-ARL and Article 20(1)2c BiBu-ARL, accountants are required to take adequate measures to establish the source of wealth and funds that are involved in the business relationship or transaction. It has to be noted that this requirement is limited to the source of wealth and funds regarding business relationships or transactions the accountant is involved in, and does not cover the whole source of wealth and funds of the customer and beneficial owners identified as PEPs (c.6.3). The accountants are required to conduct enhanced ongoing monitoring on the relationship with PEPs according to Article 37(1)2d WT-ARL and Article 20(1)2d BiBu-ARL (c.6.4).

877. From a meeting held with SROs and the professionals, the effective implementation of CDD requirements with respect to PEPs appears to be limited due to a general view that the profession is not exposed to this type of risks.

878. Pursuant to Article 37(2) WT-ARL and Article 20(2) BiBu-ARL, accountants are required to pay special attention to services and transactions that might foster anonymity (c.8.1).

879. The same articles require accountants to take measures if needed when face with such services or transactions. Some precisions on the measures to be taken are found in Article 37(1)1 WT-ARL and Article 20(1)1 BiBu-ARL. When a customer was not physically present for identification purposes, one or more of the following measures have to be taken, on the basis of a risk-oriented assessment:

- A written order should be delivered by registered letter to the address indicated by the customer. The customer should be requested to return the written order with an enclosed legible copy of an official photo identity card, which will serve for verifying the customer's data. In addition, the customer should enclose a written confirmation of a reliable warrantor concerning the authenticity of the forwarded copy. For this purpose, 'reliable warrantor' should be understood to refer to courts and other state authorities, notaries, lawyers and credit institutions, unless they have their official sphere of activity, domicile or residence in a noncooperating state;
- Upon commencement of the transaction, the first payment should be effected via an account established on behalf of the customer with an institution that is subject to Directive 91/308/EWG as amended by 2001/97/EC.

880. It has to be noted that no guidance has been issued in order for accountants to assess the risks and that there is no requirement to apply those policies when conducting ongoing due diligence (c.8.2).

881. Pursuant to Article 38 WT-ARL and Article 21 BiBu-ARL, accountants are permitted to rely on third parties to perform part of the CDD which relates to the identification and verification of the customer's and beneficial owner's identity. The ultimate responsibility for meeting those requirements remains with the accountant. The accountant must receive from the third party the necessary information, at least in the form of copies of the underlying documents, required for the fulfillment of CDD (c.9.1, c.9.2 and c.9.5).

882. According to Article 38(2)2 WT-ARL and Article 21(2)2 BiBu-ARL, third parties have to "meet the requirements set out in the Directive 2005/60/EC." This broad obligation includes Articles 14 to 19 of the Directive that cover performance of CDD by third parties. It has to be noted that no specific guidance has been given to accountants on how to satisfy themselves that the third party is regulated and supervised and has measures in place to comply with the CDD requirements (c.9.3 and c.9.4).

883. Article 41 WT-ARL and Article 24 BiBu-ARL oblige accountants to keep documents used for identification for a minimum of five years after the last business with the customer. Documents on "transactions and business relationships, vouchers and records as far as available", have also to be kept for a minimum of five years after their performance. It has to be noted that the expression "as far as available" has not been defined in any guidance. In addition, there is no requirement to keep records longer if requested by a competent authority in specific cases upon proper authority (c.10.1 and c.10.2).

884. Pursuant to Article 39(6) WT-ARL and 22(6) BiBu-ARL, accountants have to furnish the competent authority, at its request, with all information it deems necessary for the prevention or prosecution of ML. It has to be noted that, while the authorities consider that this information has to be provided without a court order, it is not generally the understanding of the accountants met by the assessors. In addition, the obligation only covers ML, not FT (c.10.3).

885. In the context of their reporting obligation, accountants are required to pay special attention to any activities and transactions which are particularly likely, by their nature, to be related to ML or FT, in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose (Article 39(2) WT-ARL and Article 22(2) BiBu-ARL). It is not clear whether this requirement is independent from the reporting obligation. There is no clarifying guidance on this (c.11.1).

886. There are no requirements to examine as far as possible the background and purpose of such transactions, to set forth their findings in writing and to keep such findings available for competent authorities and auditors for at least five years (c.11.2 and c.11.3).

#### **4.1.2. Recommendations and Comments**

887. The authorities should:

##### **All DNFBPs:**

- Review the requirements concerning PEPs.

##### **Casinos:**

- Extend the legal framework in order to cover all casinos operating in Austria;
- Establish legal requirements of CDD for internet casinos;
- Establish rules to determine the basis upon which internet casinos are subject to AML/CFT requirements;
- Set out a legal obligation for casinos to perform CDD for all customers, including non EU/EEA citizens, when they engage in financial transactions equal to or above EUR 3,000;
- Require casinos to perform specific review for higher risk categories and enhanced due diligence for higher risk customers, such as non-resident customers;
- Require casinos to put in place appropriate management systems to determine whether a potential customer, a customer or the beneficial owner is a PEP;
- Set out enforceable requirements for Internet casinos in order to address the specific risks related to non-face-to-face transactions; and
- Require casinos to keep record of transactions.

**Real estate agents, dealers in precious stones and metals, and TCSPs:**

- Effectively implement GewO requirements regarding TCSP activities; review the Chamber of commerce's business profiles of management consultant, office work (*Büroarbeiten*), and office services (*Büroservice*);
- Require to verify that any person purporting to act on behalf of the customer is so authorized;
- Absence of guidelines issued by competent authorities to determine the extent of the CDD measures on a risk sensitive basis;
- Require to perform specific review for higher risk categories and enhanced due diligence for higher risk customers, such as nonresident customers;
- Review the framework of simplified CDD measures in line with the standard;
- Require to set forth and keep findings of examination of complex and unusual transactions; and
- Effectively implement the CDD requirements.

**Lawyers and Notaries:**

- Clarify the scope of the CDD requirements;
- Eliminate the reference to risk in the requirement to identify and verify the beneficial owner;
- Require enhanced due diligence for higher-risk categories such as nonresident customers or private banking;
- Review the framework of simplified CDD measures in line with the standard;
- Adopt CDD measures concerning existing customers;
- Require lawyers and notaries to pay special attention to all complex and unusual transactions;
- Review the disposition regarding the legal privilege in order not to hamper CDD measures; and
- Issue guidance for lawyers in order to facilitate effective implementation.

**Accountants:**

- Clarify the scope of the CDD requirements;
- Eliminate the reference to risk in the general CDD requirement;
- Eliminate the reference to risk in the requirement to identify and verify the beneficial owner;
- Review the framework of simplified CDD measures in line with the standard;
- Require to set forth and keep findings of examination of complex and unusual transactions;
- Review the disposition regarding the legal privilege in order not to hamper CDD measures; and
- Effectively implement the CDD requirements.

## 4.1.3. Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	PC	<p><u>All DNFBPs:</u></p> <ul style="list-style-type: none"> <li>• Some shortcomings in the requirements concerning PEPs .</li> </ul> <p><u>Casinos:</u></p> <ul style="list-style-type: none"> <li>• Absence of AML/CFT requirements for all casinos operating in Austria.</li> <li>• No legal framework for CDD requirements concerning Internet casinos.</li> <li>• No rules to determine the basis upon which internet casinos are subject to AML/CFT requirements.</li> <li>• No legal obligation for casinos to perform CDD for all customers when they engage in financial transactions equal to or above EUR 3,000.</li> <li>• No specific review for higher risk categories and no enhanced due diligence for higher risk categories of customers, such as non-resident customers.</li> <li>• No legal obligation of record keeping of transactions.</li> <li>• No enforceable requirements for Internet casinos in order to address the specific risks related to non-face-to-face transactions.</li> <li>• No appropriate management systems to determine whether a potential customer, a customer or the beneficial owner is a PEP.</li> </ul> <p><u>Real estate agents, dealers and TCSPs:</u></p> <ul style="list-style-type: none"> <li>• Coverage of TCSP activities is not effective.</li> <li>• No requirement to verify that any person purporting to act on behalf of the customer is so authorized.</li> <li>• No guidelines issued to determine the extent of the CDD measures on a risk sensitive basis.</li> <li>• No specific review for higher risk categories and no enhanced due diligence for higher risk categories of customers, such as non-resident customers.</li> <li>• Weaknesses of the simplified CDD framework.</li> <li>• No requirement to keep written findings of the examination of complex and unusual transactions.</li> </ul>

	<ul style="list-style-type: none"> <li>• Lack of effective implementation of the CDD requirements.</li> </ul> <p><u>Lawyers and notaries:</u></p> <ul style="list-style-type: none"> <li>• The scope of the CDD requirements is unclear.</li> <li>• The identification and verification of the beneficial owner is not systematic.</li> <li>• Absence of enhanced due diligence required for higher risk categories.</li> <li>• Weaknesses of the simplified CDD framework.</li> <li>• Absence of requirements concerning existing customers.</li> <li>• No requirement to pay special attention to all complex and unusual transactions.</li> <li>• Extent of the CDD requirements is limited by the wide definition of the legal privilege.</li> <li>• Effective implementation limited by the absence of guidance for lawyers.</li> </ul> <p><u>Accountants:</u></p> <ul style="list-style-type: none"> <li>• Scope of the CDD requirements unclear for accountants regulated by the WT-ARL.</li> <li>• Limitation of the general CDD requirements due to a reference to risk.</li> <li>• The identification and verification of the beneficial owner is not systematic.</li> <li>• Extent of the CDD requirements is limited by the wide definition of the legal privilege.</li> <li>• Weaknesses of the simplified CDD framework.</li> <li>• No requirement to keep written findings of the examination of complex and unusual transactions.</li> <li>• Lack of effective implementation of the CDD requirements.</li> </ul>
--	---

## 4.2 Suspicious Transaction Reporting (R.16)

### 4.2.1 Description and Analysis

#### Legal Framework

##### Casinos:

888. The STR requirements for casinos are included in Article 25 GSpG. Additional requirements are included in the “Safety measures to prevent ML” that have been approved by the MoF. There are no STR requirements for electronic lotteries (internet casino).

##### Real estate agents, dealers and management consultants:

889. The provisions regarding the reporting of suspicious transactions and related measures are mainly included in Article 365t to 365x GewO.

##### Lawyers and Civil Law Notaries

890. According to the professional regulations for lawyers and notaries, the notary or lawyer as well as the competent regional Chamber as SRO (as part of its duty to conduct reviews) are under an obligation to report suspicions to the A-FIU (cf. Article 8c RAO; Articles 36c and Article 154 NO).

##### Chartered public accountants and tax consultants

891. Article 39, paragraph 2 and Article 42, paragraph 1, lit. b WT-ARL apply.

##### Accountancy Professions

892. Article 20, paragraph 2 and Article 25, paragraph 1, lit. b BiBu-ARL apply.

#### *Requirement to Make STRs on ML and FT to FIU (applying R. 13 & SR. IV to DNFBPs) (c.16.1)*

##### Land-Based Casinos

893. Casinos have to immediately inform the MoI if there is a suspicion or a legitimate reason to assume that a transaction of a visitor serves for ML or if a visitor of a casino is a member of a terrorist association according to Article 278b StGB or a visitor’s transaction serves for terrorism financing according to Article 278d. Due the fact that the reporting obligation includes a cross-reference to the definition of TF in the criminal code, the technical shortcomings noted in paragraphs 184–186, *infra*, could conceivably influence a casino’s decision on whether to file a report. As a practical matter, the assessors are convinced by the authorities’ explanation that the broad definition of an STR will override this largely theoretical concern. As the reference to ML can implicitly be understood as referring to Article 165 StGB, self-laundering is not included in the reporting requirement. In addition, the reporting obligation is limited to ML and is consequently narrower than the standard which mentions the funds that are proceeds of a criminal activity (c.13.1 and 2).

894. Transactions should be reported regardless of the amount of the transaction, but there is no legal requirement to report attempted transactions in Article 25 (6) GSpG (c.13.3).

895. The requirement to report suspicious transactions applies regardless of whether they are thought, among other things, to involve tax matters, as explained in section 3 regarding c.13.4.

896. The reporting requirements mentioned in GSpG implicitly refer to the transactions that are suspected to serve ML as defined under Article 165 StGB. Consequently, the requirement to report includes the laundering of the proceeds of all criminal acts that would constitute a predicate offense for ML in Austria. But the reporting obligation does not require financial institutions to report funds that are the proceeds of the criminal acts that are listed in Article 165 if there is no element demonstrating that the transaction serves the purpose of ML (additional c.13.5).

### **Internet Casinos**

897. The licensee applies a risk-based monitoring on the transactions, mostly in order to ensure responsible gaming, but this monitoring may help to detect transactions that could serve the purpose of ML or FT. This kind of transactions has never been detected. In case they were, the GSpG and the Gaming conditions do not mention any obligation to report suspicious transactions to the A-FIU.

### **Real Estate Agents, Dealers and Management Consultants:**

898. Pursuant to Article 365u(1) GewO, the designated trade persons are required to promptly inform on their own initiative, where they know, suspect, or have reasonable grounds to suspect that ML or FT is being or has been committed. According to Article 365n(1), money laundering means an offense pursuant to Article 165 StGB, consequently self-laundering is not included in the reporting requirement. In addition, the reporting obligation is limited to ML and is consequently narrower than the standard which mentions the funds that are proceeds of a criminal activity (c.13.1).

899. According to Article 365n(2) GewO, terrorist financing means the provision of a financial contribution to support a terrorist group pursuant to Article 278b StGB, to commit a terrorist offense pursuant to Article 278c StGB or to complete the offense pursuant to Article 278d StGB. The reporting obligation covers the obligation to report where there is a suspicion that the funds support terrorist organizations, or those who finance terrorism even when there is no link to a terrorist act. Indeed, the definition of a terrorist group in Article 278b is broad and, by reference to Article 278(3), StGB includes the participation by providing assets with the knowledge that it supports the organization or its criminal acts (c.13.2, c.IV.1).

900. The reporting obligations apply irrespective of any threshold and Article 365u(1) GewO covers attempted (“*zu begehen versucht*”) transactions (c.13.3) The requirement to report suspicious transactions applies regardless of whether they are thought, among other things, to involve tax matters, as explained in Section 3 regarding c.13.4.

### **Lawyers and Notaries**

901. Pursuant to Article 8c(1) RAO and 36c(1) NO, lawyers and notaries have to immediately inform the BKA if they know, suspect, or has a well-founded reason to suspect, that the transaction serves the purpose of ML (Article 165 StGB). Consequently, self-laundering is not included in the

reporting requirement. In addition, the reporting obligation is limited to ML and is consequently narrower than the standard which mentions the funds that are proceeds of a criminal activity. The lawyers and notaries are not obliged to report suspicions with regard to information they receive from, or obtain on, one of their clients, when providing legal advice or when representing the client before court or before a preceding authority or public prosecution office—unless the client has evidently made use of the legal advice for the purpose of ML or FT (c.13.1).

902. The same reporting obligation applies in the case of terrorism financing (Article 278d StGB). Due to the fact that the reporting obligation includes a cross-reference to the definition of TF in the criminal code, the technical shortcomings noted in paragraphs 184–186, *infra*, could conceivably influence a lawyer or a notary’s decision on whether to file a report. As a practical matter, the assessors are convinced by the authorities’ explanation that the broad definition of an STR will override this largely theoretical concern.(c.13.2).

903. The RAO and the NO do not mention any threshold concerning the reporting obligations and include attempted transactions (c.13.3).

904. The requirement to report suspicious transactions applies regardless of whether they are thought, among other things, to involve tax matters, as explained in section 3 regarding c.13.4.

### **Chartered Public Accountants, Tax Consultants and Accountancy Professions**

905. Pursuant to Article 39(2) WT-ARL and Article 22(2) BiBu-ARL, chartered public accountants and tax consultants are required to promptly inform the A-FIU, on their own initiative, if they know, suspect or have reasonable grounds to suspect that ML or FT within the meaning of the StGB is being or has been committed. Self-laundering is not included in the reporting requirement. In addition, the reporting obligation is limited to ML and is consequently narrower than the standard that mentions the funds that are proceeds of a criminal activity. It has to be noted that Article 39(1) WT-ARL and Article 22 (1) precise that accountants may report to the authority “only after having carefully assessed all circumstances.” In addition, according to Article 39(6) WT-ARL and Article 22(6) BiBu-ARL, the reporting obligation does not apply to information accountants receive from or obtain on one of their clients in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in or concerning judicial or other official proceedings, including advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings. However, the reporting obligation remains in force if the accountant knows that the client uses the legal advice intentionally for the purpose of ML or FT (c.13.1).

906. Article 39(2) WT-ARL and Article 22(2) BiBu-ARL also oblige to make an STR when accountants know, suspect or have reasonable grounds to suspect that FT is being or has been committed within the meaning of the StGB. Due to the fact that the reporting obligation includes a cross-reference to the definition of TF in the criminal code, the technical shortcomings noted in paragraphs 146–148, *infra*, could conceivably influence an accountant’s decision on whether to file a report. As a practical matter, the assessors are convinced by the authorities’ explanation that the broad definition of an STR will override this largely theoretical concern (c.13.2).

907. The WT-ARL and the BiBu-ARL require reporting attempted transactions but do not clearly require to report in case they have suspicions on occasional transactions amounting to less than EUR 15,000 (c.13.3).

908. The requirement to report suspicious transactions applies regardless of whether they are thought, among other things, to involve tax matters, as explained in section 3 regarding c.13.4.

909. Overall, the level of reporting of the designated trade persons is evenly low (see table below). This situation can be explained by the still recent addition of those professions in the AML/CFT framework and the necessity of more training. Another possible explanation, more structural and already mentioned for financial institutions regarding c.13.1, is the structure of the criminal procedure in Austria. When a reporting entity sends an STR, it knows that the suspected person could ultimately know that it was denounced. This may be a severe impediment to report, especially for professions with a small size where it is quite easy for the criminal to know exactly the person that made the report. In addition, the advocated advantages of the flexible relation between the A-FIU and the financial reporting institutions are less evident in the case of DNFBPs. Indeed, it relies on trust and constant exchange of information, which is not possible to achieve with all DNFBPs, the total number of which counts in tens of thousands, or in hundreds of single entities for the most active or at risk.

Statistical Table 30. STRs filed by DNFBPs

	2004	2005	2006	2007
<b>Casinos</b>	2	1	0	1
<b>Lawyers</b>	1	4	4	1
<b>Notaries</b>	2	3	2	3
<b>Accountants</b>	0	0	1	1
<b>Real Estate Agents</b>	0	1	0	1
<b>Dealers</b>	3	1	3	4
<b>TCSPs</b>	0	2	2	2
<b>Total</b>	<b>8</b>	<b>12</b>	<b>12</b>	<b>13</b>

***Appropriate cooperation forms between SROs and the FIU (c.16.2)***

910. There are four types of SROs in Austria: the Bar Association, the Chamber of Notaries, the Economic Chamber for chartered Public Accountants and Tax Consultants, and the Parity Commission for the Accountancy Professions. None of these SROs are established as bodies that have to be informed in the first instance in place of the A-FIU. For lawyers, notaries and accountants, the STR has to be sent to the BKA/A-FIU. However, Article 8c(1a) RAO and Article 36c(1a) NO allow the lawyer and the notary to inform their respective SROs.

***Applying R.14, R.15 and R.21 to DNFBPs (c.16.3)***

### **Land-Based Casinos**

911. Pursuant to Article 25(6) GSpG, Article 41(7) BWG applies to casinos. Consequently, claims for damages should not be permitted based on the circumstance that a casino, or its employees, delayed or failed to execute a transaction on the negligent lack of knowledge that the suspicion of ML or terrorism financing was wrong. The notion of employees covers every staff in contractual relation with a casino, including directors (c.14.1).

912. Pursuant to Article 25(6) GSpG, Article 41(3b) BWG applies to casinos. It could be referred to the description and analysis of R.14 in section 3 for more details on the limits to the prohibition from disclosing to third parties (c.14.2).

913. Concerning Recommendation 15, pursuant to Article 25a GSpG, Article 41 (4) BWG applies to casinos. It could be referred to the description and analysis of R.15 in section 3 for more details on the legal framework. A compliance officer has been nominated to cover ML/FT-purposes for CASAG and ÖLG. He/she is in particular in charge of setting up internal policies and raising awareness. He/she has a direct access to customer identification data and other CDD information and transactions records. The position is now distinct from the responsible for gaming and tries to address the specificities of the ML/FT risk. The compliance officers visit to casinos to train staff, including top management and staff in charge of the entrance and of the payments. They operate in coordination with the internal audit, particularly in charge of the verification of the handling of money, but that has been trained on AML/CFT issues. One four person team of the internal audit is in charge of making surprise visits. The compliance officer is also in charge of an AML/CFT hotline that operates 24/7. In addition, background checks are made when hiring new employees. In CASAG, the compliance officer reports to the head of the legal and European affairs department.

914. Concerning Recommendation 21, there are currently no specific requirements to give special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations. The authorities consider that it is part of the risk based approach. In this context, information such as the FATF International Cooperation Review Group (IRCG) process has to be taken into account.

### **Internet Casinos**

915. The legal framework does not establish any requirements in relation to R. 14, R.15 and R.21. Concerning R.15, the licensee has a special “fraud and collusion” team that has been trained on ML/FT. Concerning R.21, the extent of application would be limited to foreign persons residing in Austria, as the residence criteria is a pre-condition to play on-line.

### **Real Estate Agents, Dealers, Management Consultants and Insurance Intermediaries**

916. According to Article 365u(2) GewO, the reporting of suspicion by the designated trade and business persons should not constitute a breach of any restriction on disclosure of information imposed by contract, or by any legislative, regulatory or administrative provision, and should not lead to a liability of any kind. There is no mention on the necessity to have reported in good faith to the A-FIU (c.14.1).

917. Article 365x (1) GewO determines that the tradespersons, and where applicable, their directors and employees should not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Article 365u GewO or that a ML or FT investigation is being or may be carried out. Pursuant to Article 365x(2) GewO, this prohibition does not include the competent authorities or disclosure for law enforcement purposes. There is no definition of competent authority (c.14.2).

918. Due to the specificity of the Austrian criminal procedure (see the analysis for R.13 and R.14 in section 3), it is possible that the STR will ultimately be known from the reported person (additional element - c.14.3).

919. Pursuant to Article 365z (1) GewO, the designated tradespersons have to establish adequate and appropriate policies for customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to ML or FT. These provisions are recent and do not appear currently implemented across the trade business. In addition, in the absence of a structured risk assessment for these professions undergone and circulated by the authorities, it is difficult for the tradespersons to determine when adequate and appropriate policies are required. The authorities consider that “adequate and appropriate” means that the type and extent of the listed measures should be based on the risk of ML and FT and the size of the business. The authorities consider that Austrian enterprises in general are very small with hardly more than five employees, so in practice a compliance officer is not as relevant as for example credit institutions. Consequently, there is no general and mandatory requirement to develop appropriate compliance management arrangements (c.15.1), audit function (c.15.2) and ongoing employee training (c.15.3).

920. Pursuant to Article 265z(2) GewO, the designated tradespersons have also to take appropriate measures so that their relevant employees are aware of the provisions in force on the prevention of the use of the financial system for the purpose of ML and FT. This includes also the participation of employees in special ongoing training programs to help them recognize operations and to instruct them as to how to proceed in such cases. The MoI has to inform the WKO on the practices of money launderers and terrorist financiers and on indications leading to the recognition of suspicious transactions. These provisions are also new and do not appear currently implemented across the trade business. Some meetings with the A-FIU were organized by regional chamber of commerce, like in Vorarlberg and Styria. The WKO also receives general information from the A-FIU on cases regarding phishing, fraud or articles of newspapers based on STRs (c.15.3).

921. There is no mention of specific screening procedures in the GewO to ensure high standards when hiring employees, in the context of the fight against ML and FT. But according to the general provisions of the GewO (Article 13(1) GewO), natural persons have to be excluded from carrying on any trade or business if they have been sentenced by any court, particularly for any criminal offense to a term of imprisonment of more than three months or a fine of more than 180 daily rates and the sentence has not yet been removed from the criminal record (c.15.4).

922. Article 365t GewO mentions that tradespersons have to pay special attention to any activity which they regard as particularly likely to be related to ML or FT. But no regulation requires the designated tradespersons to give special attention to business relationships and transactions with

persons from or in countries which do not or insufficiently apply the FATF Recommendations (c.21.1 and c.21.2).

### **Lawyers and Civil Law Notaries**

923. According to Article 9(5) RAO and 37 (5) NO, the reporting of suspicion by a lawyer or a notary in good faith should not constitute any breach of any restriction on disclosure of information imposed by contract, or by any legislative, regulatory or administrative provision, and should not lead to a liability of any kind. (c.14.1).

924. The notary or the lawyer may only inform the authorities responsible for the fight against ML and FT, the SRO and the public prosecution authorities of reported suspicions or notifications to the MoI (Federal Office of Criminal Investigations) pursuant to Article 36b NO and 8b RAO (prohibition to disclose information). Such information may, however, also be passed on within a notarial or lawyer's office or partnership (Article 36c(1a) NO and 8c(1a) RAO. In addition, pursuant to Article 8c(1a) RAO and Article 36c(1a) NO, the prohibition to transmit information does not prevent the lawyer or the notary from efforts to deter the party from committing an unlawful act. If the party has contracted services of another lawyer or notary in a EU Member State or a third country in which similar requirements and similar secrecy and data protection provisions apply as in Directive 2005/60/EC, or if this lawyer or notary is involved in the party's transaction, information relating to the transaction may be passed on. The information exchanged may only be used to prevent ML or FT. Article 8c(1a) RAO and Article 36c(1a) NO only apply to the disclosure of STR. There are no specific requirements in relation to information disclosed to the BKA in relation to Article 9(4) RAO and Article 37(4) NO. In this case, Article 9(2) RAO and Article 37(1) NO apply, lawyers and notaries are bound to secrecy in respect of all business transacted in his presence vis-à-vis the parties (c.14.2).

925. Due to the specificity of the Austrian criminal procedure (see the analysis for R.13 and R.14 in section 3), the STR can ultimately be known from the reported person (additional element - c.14.3).

926. Pursuant to Article 36a(2) RAO and 8a(2) NO, lawyers and notaries are required to establish and maintain internal procedures, policies and controls to prevent ML and FT and to communicate them inside their firms. The designation of an AML/CFT compliance officer is not made mandatory in a firm (c.15.1). The firms are not required to maintain an adequately resourced and independent audit function to test compliance with the procedures, policies and controls to prevent ML and FT. The authorities consider that these measures might be appropriate for financial institutions of a certain size, but with regard to law or notarial firms it has to be taken into account that they are usually much smaller than financial institutions (c.15.2). Pursuant to Article 21b(2) RAO and Article 117(1) NO, lawyers and notaries are required to establish training to familiarize employees with the provisions serving to prevent or fight ML or FT. Such measures include inter alia enrolment of the lawyers and notaries in special training programs (c.15.3).

927. The AML/CFT provisions of the RAO and the NO do not provide for specific screening procedures to ensure high standards when hiring employees. But, concerning lawyers (Article 5(2) RAO), their registration has to be denied if they have acted in a way making them "unworthy of trust." As per notaries (Article 6(1) and Article 7(2) NO), they can only be appointed if they are of "good character" and are prohibited to engage in any activity which is incompatible with the dignity

and honor of the profession, or which may undermine the full trust in their objectivity or the credibility emanating from the deeds they draft (c.15.4).

928. Lawyers or notaries are not specifically required to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations (c.21.1 and c.21.2).

### **Chartered Public Accountants and Tax Consultants and Accountancy Professions**

929. Pursuant to Article 39(8) WT-ARL and Article 22(8) BiBu-ARL, the reporting of suspicion by an accountant in good faith should not constitute any breach of any restriction on disclosure of information imposed by contract, or by any legislative, regulatory or administrative provision, and should not lead to a liability of any kind for the accountants, their managerial staff or their employees (c.14.1).

930. Accountants, as well as managerial staff and employees of firms are prohibited to disclose to the customer or to third persons the fact that a STR or related information has been transmitted to the A-FIU or that a ML or FT investigation is being or may be carried out (Article 4,(1) WT-ARL and Article 23(1) BiBu-ARL). This prohibition does not apply to non-national accountants who perform their professional activities within the same company or network. “Network” is to be considered as the larger structure to which these persons belong and which shares common ownership, management or compliance control with respect to the provisions for preventing ML and FT (Article 40(2) WT-ARL and Article 23(2) BiBu-ARL). Information may disclosed exclusively for the purpose of preventing ML and FT to other, including non-national persons entitled to practice said professions, provided that the matter concerns the same customer and the same transaction involving these persons entitled to practice said professions. Any disclosure of information to non-national persons entitled to practice said professions should only be permitted if the latter are subject to requirements equivalent to those of the present chapter as well as to equivalent obligations with regard to professional secrecy and the protection of personal data (Article 40(3) WT-ARL and Article 23(3) BiBu-ARL). Finally, pursuant to Article 40(3) WT-ARL and Article 23(3) BiBu-ARL, seeking to dissuade a customer from engaging in illegal activity is not considered as a disclosure to the customer (c.14.2).

931. Due to the specificity of the Austrian criminal procedure (see the analysis for R.13 in section 3), the STR can ultimately be known from the reported person (additional element–c.14.3).

932. Pursuant to Article 42(1) WT-ARL and Article 25(1) BiBu-ARL, accountants are required to establish adequate and appropriate policies and procedures to prevent ML and FT. These procedures should cover CDD, record keeping, reporting of suspicions, risk assessment and risk management with respect to business relationships and transactions, as well as suitable control and information systems at their offices. There is no requirement to designate an AML/CFT compliance officer at firm’s level (c.15.1). The authorities consider that, in practice, accountancy services are offered by single professionals or very small offices/companies where the establishment of a compliance officer would be an excessive requirement.

933. Accountants are not required to maintain, at firm’s level, an adequately resourced and independent audit function to test compliance with the procedures, policies and controls to prevent ML and FT (c.15.2).

934. Pursuant to Article 42(2) WT-ARL and Article 25(2) BiBu-ARL, accountants are required to familiarize the personnel employed at their offices with the provisions aimed at preventing and combating ML and FT and ensure their participation in special training programs. There is no specific requirement to keep the employees informed of new developments, including information on current ML and FT techniques, methods and trends (c.15.3).

935. Accountants are not required to put in place specific screening procedures to ensure high standards when hiring employees. The articles relating to the hiring of staff (Article 8(1) BiBu) only mentions the need to examine candidates “for their professional and personal aptitudes” (c.15.4).

936. Accountants are not required to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations (c.21.1 and c.21.2).

***Extension of the reporting requirement to the rest of the professional activities of accountants (additional element – c. 16.5)***

937. The reporting requirement of accountants extends to all activities of accountants, including auditing pursuant to Article 32(2) WT-ARL and Article 15(2) BiBu-ARL.

**4.2.2. Recommendations and Comments**

The authorities should take the following actions regarding the different DNFBPs:

**All DNFBPs:**

- Align the grounds for reporting on the standard.
- Give special attention to business relationships and transactions with persons from countries insufficiently applying the FATF recommendations.

**Casinos:**

- Require Internet casinos to report STRs and specify AML/CFT internal controls.

**Real estate agents, dealers and TCSPs:**

- Effectively extend the legal obligation to report STRs and have internal control in place to all businesses and professions conducting TCSP activities.

**Lawyers and notaries:**

- Consider reviewing the matters that fall under legal professional secrecy of notaries and lawyer, that currently appear very broad.

**Accountants:**

- Consider reviewing the matters that fall under legal professional secrecy of accountants, which currently appear very broad.

### 4.2.3. Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	PC	<p><u>All DNFBPs</u></p> <ul style="list-style-type: none"> <li>• Scope of STRs too narrow.</li> <li>• Effectiveness questions raised by the extremely low level of STRs.</li> <li>• No requirements to give special attention to business relationships and transactions with persons from countries insufficiently applying the FATF recommendations.</li> </ul> <p><u>Casinos</u></p> <ul style="list-style-type: none"> <li>• No requirements for internet casinos.</li> </ul> <p><u>Real estate agents, dealers and TCSPs</u></p> <ul style="list-style-type: none"> <li>• Absence of effective coverage of TCSPs.</li> </ul> <p><u>Lawyers and notaries</u></p> <ul style="list-style-type: none"> <li>• Scope of the legal privilege severely limiting the requirement to report STRs.</li> </ul> <p><u>Accountants</u></p> <ul style="list-style-type: none"> <li>• Scope of the legal privilege severely limiting the requirement to report STRs.</li> </ul>

## 4.3 Regulation, Supervision, and Monitoring (R.24-25)

### 4.3.1 Description and Analysis

#### Legal Framework

#### Casinos

938. Pursuant to Article 13(1) GewO, casinos and electronic lotteries need licenses granted by the MoF according to Article 14(1) GSpG for lotteries, including electronic lotteries and Article 21(1) for Casinos covered by the State Monopoly. Licensees are supervised by the MoF pursuant to Article 19 GSpG for lotteries and Article 31GSpG for Casinos.

### Real estate agents, dealers and management consultants

939. Pursuant to Article 365m(4) GewO, the local district authority mentioned in Article 333(1) is the authority of first instance regarding the monitoring and supervision, including sanctioning infringements of AML/CFT requirements. The relevant sanctions are contained in Articles 366, 367 and 370 GewO.

### Lawyers

940. For lawyers, monitoring and ensuring compliance with AML/CFT requirements and measures are primarily governed by the RAO and the Disciplinary Statute for lawyers and lawyer-candidates (*Disziplinarstatut – DSt*, Federal Law Gazette Nr. 474/1990). Besides, there are statutory regulations set down in the Directives of the Austrian Bar Association, in the first place the Directive on the practice of the lawyers' profession and the supervision of the lawyers' duties (*Richtlinien für die Ausübung des Rechtsanwaltsberufs und für die Überwachung der Pflichten des Rechtsanwaltes – RL-BA 1977*).

### Civil Law Notaries

941. The MoJ has ultimate authority to supervise the notarial system in Austria; the presidents of courts of first-instance and second-instance have responsibility for supervising the practice of the profession by notaries. The regional Chambers of Civil Law Notaries (SRO) are first and foremost called upon to monitor notaries in the exercise of their business as well as their proper conduct (cf. Article 153 NO).

### Chartered Public Accountants and Tax Consultants

942. The competent supervisory authority is the Chamber of Chartered Public Accountants and Tax Consultants.

### Accountancy Professions

943. The competent supervisory authority is the Parity Commission for the Accountancy Professions.

Statistical Table 31. AML/CFT Regulation and Supervision of DNFBPs

<b>DNFBP</b>	<b>Supervision/Monitoring</b>	<b>Regulation</b>
<b>Casinos</b>	MoF	MoF
<b>Real estate agents</b>	Local district authorities (+ Federal Police Article 336)	MoE
<b>Dealers in precious metals and stones</b>	Local district authorities (+ Federal Police Article 336)	MoE
<b>Lawyers</b>	Bar Association	MoJ
<b>Notaries</b>	Chamber of Civil Law Notaries	MoJ
<b>Accountants</b>	MoE/Chamber of Chartered Public Accountants and Tax Consultants/Parity Commission for the	MoE

	Accountancy Professions	
TCSPs	Local district authorities (+ Federal Police Article 336)	MoE

***Regulation and Supervision of Casinos (c. 24.1)***

***Responsibility for the AML/CFT regulation, supervision and sanction (c.24.1.1)***

**Land-Based Casinos**

944. The MoF is in charge of the regulation and supervision of the casinos that are regulated by the GSpG. No AML/CFT requirements and supervision applies for casino operating outside the GSpG, including those regulated and supervised at the local level. It should be noted that the July 2008 amendments to the GSpG, introduced a new Article 25(6) that apply Article 41(4)BWG to the licensee. Pursuant to the 5<sup>th</sup> point of this Article, casinos must allow the FMA to review the effectiveness of systems for the suppression of ML or FT at any time.

945. The MoF has powers to supervise the implementation of the AML/CFT requirements in the 12 licensed casinos. Sanctions are mentioned in Article 23 and 52 GSpG. In case of breach of Article 25 which includes all AML/CFT related requirements, with the exemption of internal monitoring and training that are covered in Article 25a, the MoF can issue an order to the Casino, forbid the managers of the license from continuing to manage the license, and withdraw the license. Pursuant to Article 52.8 GSpG, an administrative offense punishable with fines up to EUR 22,000 is committed by persons responsible for a casino and violates the duties laid down in Article 25.6 to 8. This article refers to the obligations of reporting STRs and the identification of the beneficial owner. The sanctions are available to the directors and senior management, not to legal persons, with the exception of the withdrawing of the license.

946. In addition, pursuant to Article 25.8 GSpG, if the MoF has a suspicion or a legitimate reason to assume that a transaction serves for ML or FT, it has to immediately inform the MoI. This is a new provision following the July 2008 amendments to the GSpG.

947. It is also worth mentioning that the State Commissioner appointed by the MoF supports the supervisory functions of the MoF by attending all meetings of the supervisory board and the general shareholder meeting of the licensees and reports to the MoF.

948. The supervision of casinos is generally done by one single inspector of the MoF, in charge of the supervision of the 12 casinos. Each casino is inspected during operating hours in order to check compliance with obligations including AML/CFT measures required by the GSpG. An inspection generally lasts for 6 to 10 hours, with 1 to 2 hours dedicated to AML/CFT measures. The inspector then reports to the MoF. A check-list and supplementary documents have to be attached. The MoF is empowered to apply administrative sanctions. Each casino is supervised once a year. No sanction has been pronounced in the last ten years, for AML/CFT or other breaches.

949. Additionally, a specific department of the Local Tax Authority for Fees and Transaction Taxes (*Finanzamt für Gebühren und Verkehrssteuern*) checks each casino for proper determination of the tax base. This task is mainly executed by checking video recordings but also includes on-site inspections in casinos during operating hours applying a sample method. These measures contribute

to ensuring AML/CFT compliance. The tax authority reports to the MoF quarterly. No report has triggered supervisory measures for breach of AML/CFT compliance.

950. Further, the MoF requires by administrative order the casino licensee to establish a special security department (*Interne Systemkontrolle*) for controlling internal technical and security procedures. For this purpose, inspectors of the licensee perform on-site inspections in casinos during operating hours. The *Interne Systemkontrolle* has to report to the MoF quarterly, thus supporting compliance with AML/CFT measures.

### **Internet Casino**

951. The internet casino is supervised by the MoF, as part of the general supervision of the licensee in charge of the lottery, pursuant to Article 19(1) GSpG. In the absence of legal provisions regarding ML/FT requirements for lotteries, the supervisor has no legal basis to ensure that AML/CFT measures are implemented in the Internet Casino. The authorities consider that the risk of misuse of electronic lotteries for purposes of ML/FT is very low and that legal regulation does therefore not seem necessary at present. But the assessors are of the view that that Recommendation 24 does not mention the possibility to take risk into account when determining the extent of the supervision of casinos. In addition, the weaknesses noted in client identification present a risk.

#### ***Licensing of casinos by a designated competent authority (c.24.1.2)***

952. Casinos and Electronic Lotteries that are authorized to perform under the game monopoly require licenses granted by the MoF.

#### ***Prevention against criminals (c.24.1.3)***

953. The MoF is in charge of taking the legal and regulatory measures to prevent criminals controlling casinos.

954. The conditions to grant a license are listed in Articles 14 (lotteries) and 21 (casinos) GSpG. It includes the absence of criminal records of managers, the absence of “shareholders who exercise a dominating influence and whose influence might be detrimental to the reliability with regard to public order.” The law does not require performing any particular control on the beneficial owner of a significant of controlling interest, and does not focus on the risk posed by the associations of criminals. But the authorities mentioned that, in practice, there were only few changes in ownership of the licensee since 1967 and if so, shares were sold only to other current shareholders. Shareholders are the Federal State (Austrian Mint), Austrian banks and insurances as well as a few private owners since more than 40 years.

955. Additionally, all shares of the licensee have to be deposited at a licensed credit institution. The MoF can block any changes in shareholding and has to be informed on the shareholders’ identity by the licensees once a year. Any appointment of new members of the executive board and any new president of the supervisory board and its deputy are subject to prior approval by the MoF. One member of the supervisory board of the electronic lotteries is appointed at the proposal of the MoF (Article 19, paragraph 3 GSpG). Licensees are required to submit the audited annual statements,

annual reports and annual statement of the group as well as the annual audit reports on these reports to the MoF within 6 months of the end of the fiscal year (Article 19, paragraphs 4 and 31, paragraph 3 GSpG). Employees of the licensee are not allowed to acquire any shares of the licensee (Article 27, paragraph 2 GSpG). The MoF can further block the acquisition of qualified investments by the Licensees (Article 15, paragraphs 1 and 24, paragraph 1 GSpG).

956. It should be noted that the current structure of ownership of CASAG, the company that holds the 12 casino licenses and the lottery license appears transparent. Its shareholders are the Federal State (Austrian Mint) for one third, Austrian banks and insurance companies for one third, the rest being mostly historical individual shareholders.

#### ***Monitoring Systems for Other DNFBPs (c. 24.2)***

957. The authorities have not performed a comprehensive risk assessment that would enable them to determine whether the system for monitoring and ensuring compliance of the other DNFBPs is appropriate. There is currently no documented risk analysis for each of the sectors that would help determine the extent of required measures<sup>42</sup>.

#### **Real Estate Agents, Dealers and Management Consultants**

958. The authorities in charge of monitoring and ensuring the compliance of real estate agents, dealers and management consultants with AML/CFT requirements are the local district authorities (there are 120 districts). The local district authority is in charge of the trade inspection functions. In places having federal police offices, these should help the local district authorities. They can report to the trade authorities any information raising doubts as to the reliability of the persons concerned when reliability checks are required (Article 336a(1) GewO) or help enforce the measures necessary for the beginning of administrative penalty procedures (Article 336(1) GewO). According to the authorities, the police can support the monitoring of AML/CFT requirements. But there is currently no specific cases of cooperation (c.24.2.1).

959. According to Article 365m (4) GewO, the local trade authorities are responsible for continually monitor and ensure compliance by trade and business persons with the Article of the GewO relating to the preventive measures against ML and FT (Article 365m to 365z), including sanctioning any infringements of these provisions. The trade authorities have to monitor compliance with the provisions on a risk-sensitive basis and take the measures necessary to ensure such compliance. They are also granted the power to compel the production of any information that is relevant for the monitoring the compliance with pertinent provisions and perform on-site inspections and checks. Article 366 GewO provides that any infringement of the obligation in Article 365u to promptly inform the A-FIU, or to furnish the necessary information and documents is to be punished by a fine up to EUR 3,600. Article 367 GewO provides that an infringement of the provisions of Article 365m to 365z GewO concerning measures on the prevention of ML and FT is to be punished by a fine up to EUR 2,180. Finally, also the permission to trade can be cancelled. Article 370 GewO provides that fees can also be imposed on legal persons or registered companies for infringements

<sup>42</sup> After a high-level meeting on November 19, 2008, the MoE sent a letter to the MoI (BKA) requesting to inform trade authorities on any local or sector-specific risk of ML/FT.

referred to in Article 365m to 365z which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person or registered company, who has a leading position within the legal person. Legal persons or registered companies can also be held liable, where the lack of supervision or control by a person referred to above has allowed for the commission of infringements for the benefit of a company by a person under its authority (c.24.2.1.a).

960. According to the authorities, approximately 100 visits have been performed by the local district authorities since 2002, including 91 in Vienna only. No sanction has ever been pronounced. In one region written warnings on compliance were delivered. The size of the inspection teams varies depending on the size of the districts. In Vienna, the trade inspection has a staff of 70, and there is a four person competence group specialized in difficult rules under the Trade act, including AML/CFT requirements. The trade inspectors have been trained to AML/CFT in January 2008. Ninety-one inspections have been performed randomly during the last three years. There is currently no risk-based monitoring and the specific risks of each profession have not been extensively studied. It also appears clearly that there is a problem of resources, in terms of staffing and expertise in criminal and financial issues. There is also an apparent interest in making the standards consistent for controls across Austria, but currently these depend totally on the priorities of the local district authorities<sup>43</sup> (c. 24.2.1.b).

961. A meeting of the heads of trade authorities of the nine Austrian States which took place in Krems in September 2008, identified several issues that would require final decision in another meeting expected in the near future. This includes the finalization of a checklist for the execution of controls, and an Austrian wide strategy on the activities of the authorities. This should address concrete ML/FT threats based on information from the police authorities or trade authorities. Additionally, decisions will be taken on the way of cooperation between central units and non-central units as well as between the police authorities and the trade authorities.

## Lawyers

962. The Board of the Bar Association (*Ausschuss der Rechtsanwaltskammer*) in Austria, where the lawyer is registered in the list of lawyers, is the responsible authority (SRO) for monitoring his/her compliance with the professional regulations including the AML/CFT requirements and measures (Article 1, paragraph 3 DSt, Article 23, paragraph 2 RAO). Within its scope, the Bar Association has to take care of, support and represent the professional, social and economic interests of the lawyers. The Bar Association is also in charge of protecting the honor, image, rights and independence of the profession, as well as monitoring compliance with the obligations of the lawyers (Article 23(2) RAO). The members of the Board are elected by the members of the Bar Association for a term of three years (Article 24 RAO). Disciplinary offenses are to be handled by the Disciplinary Council (*Disziplinarrat*) established by each Bar Association in Austria (Article 1, paragraph 2 DSt). A violation of AML/CFT obligations can be referred to the Board of the Bar Association or the Disciplinary Council. It can be taken up because of a complaint or ex officio (Article 22 DSt) and is then dealt with according to the disciplinary procedure. The Disciplinary

---

<sup>43</sup> The November 2008 meeting also decided to create a checklist for on-site controls and a strategy on risk-based supervision. Those documents have been distributed to all local district authorities.

Council consists of lawyers who are elected by the members of the Bar Association for a term of three years (Article 7 DSt). Furthermore a bar lawyer (*Kammeranwalt*) is appointed according to Article 5 DSt, who has to investigate in disciplinary cases in order to bring them before the Disciplinary Council.

### **Civil Law Notaries**

963. The competent regional Chamber of Civil Law Notaries (SRO) is obliged to examine the files of notaries within its remit to review their business activities from time to time. This includes verifying whether notaries comply with the provisions serving to prevent or fight ML or FT. If the regional Chamber of Civil Law Notaries detects facts related to ML or FT, it must report its suspicion to the A-FIU (cf. Article 154 NO). If a notary violates a statutory obligation in the context of AML/CFT (imposed e.g., by the NO), he/she is in breach of a professional duty that will be sanctioned as a major disciplinary offense by the higher regional court as the disciplinary court after a hearing by the senior public prosecutor, or as a minor disciplinary offense by the competent regional Chamber of Civil Law Notaries (cf. Article 155 NO).

### **Chartered Public Accountants and Tax Consultants**

964. The Chamber of Chartered Public Accountants and Tax Consultants is in charge of monitoring the profession and is subordinated to the MoE. (Articles 145-162 WTBG). Detailed duties and responsibilities are described in Article 146 WTBG. The Chamber of Chartered Public Accountants and Tax Consultants is the official professional representation for the chartered public accountants and tax consultants with a magisterial character. Natural and legal persons under the WTBG are registered in the register and are being supervised by this authority as well as by the MoE. A requirement to be registered is for the enterprises, respectively their legal representative, to be free of former convictions for crimes.

### **Accountancy Professions**

965. The Parity Commission for the Accountancy Professions is in charge of monitoring the profession and is subordinated to the MoE. Detailed duties and responsibilities are described in Articles 91-95 BiBuG.

### ***Designated competent authority or SRO (c. 24.2.1)***

#### **Lawyers**

966. The Board of the Bar Association (*Ausschuss der Rechtsanwaltskammer*) in Austria, where the lawyer is registered in the list of lawyers, is the responsible authority (SRO) for supervising his/her compliance with the professional regulations including the AML/CFT requirements and measures (Article 1, paragraph 3 DSt, Article 23, paragraph 2 RAO). Within its scope, the Bar Association has to take care of, support and represent the professional, social and economic interests of the lawyers belonging to the Bar Association. The Bar Association is also obliged to protect the honor, image, the rights and the independence as well as to monitor the obligations of the lawyer's profession (Article 23(2) RAO). The members of the Board are elected by the members of the Bar Association at their plenary session for a term of three years (Article 24 RAO). Disciplinary offenses

are to be handled by the Disciplinary Council (*Disziplinarrat*) established at each Bar Association in Austria (Article 1, paragraph 2 DSt). The Disciplinary Council consists of lawyers who are elected by the members of the Bar Association for a term of three years (Article 7 DSt). Furthermore a bar lawyer (*Kammeranwalt*) is appointed according to Article 5 DSt, who has to investigate in disciplinary cases in order to bring them before the Disciplinary Council. The visits are conducted either on the basis of a suspicion or randomly. During the visits, it is possible to ask for files, copies of correspondence or bank accounts.

967. The Supreme Appeals and Disciplinary Commission (*Oberste Berufungs- und Disziplinarkommission, OBDK*) is the court of appeal against decisions of the Disciplinary Council. It consists of two judges of the Supreme Court (*Oberster Gerichtshof*) and two lawyer judges, whereas always a judge of the Courts of Appeal acts as chair.

968. Decisions of the Disciplinary Council and the Supreme Appeals and Disciplinary Commission are executed by the Board of the competent Bar Association (Article 67 DSt). If a lawyer has been removed from the list or prohibited to work as a lawyer, the Board has to inform the Ministry of Justice, the president of the Supreme Court, the Constitutional Court, the Administrative Court and the Courts of Appeal about the disciplinary measures imposed upon the lawyer (Article 70 DSt). Furthermore these circumstances have to be published on the web site of the Austrian Bar Association ([www.rechtsanwaelte.at](http://www.rechtsanwaelte.at)) and in the Austrian Lawyers' Journal (*Österreichisches Anwaltsblatt*). In other cases, only relevant courts or administrative authorities have to be informed. The MoJ has supervisory rights ensuring the orderly course of the disciplinary proceedings (Article 78 DSt).

969. The Disciplinary Council may impose sanctions ranging from written warnings, to fines up to EUR 45,000 and the debarring from the lawyers' profession for up to one year, up to the deletion from the list of lawyers (Article 16 DSt). The Disciplinary Council may also resolve interim measures against a lawyer when:

- criminal proceedings are held against him/her;
- the lawyer has been found guilty of a criminal act by a court;
- the disciplinary measure of removal from the list of lawyers has been imposed; or
- a request to open insolvency proceedings has been made against the lawyer.

970. Interim measures are the supervision of the law firm management through the Board of the Bar Association, the exclusion of the right to represent before specific or all courts or administrative bodies, the interim interdiction to admit trainee lawyers for traineeship and even the interdiction of the exercise of the lawyer's profession (Article 19 DSt). This system of disciplinary supervision and sanctions thus guarantees effective, proportionate and dissuasive sanctions with regard to lawyers that fail to comply with national AML/CFT requirements. It can ensure that lawyers comply with their obligations to combat ML and FT.

971. The Disciplinary Council has to report to the public prosecutor, in case the disciplinary offense the lawyer is accused of constitutes a suspicion of a criminal act (Article 23 DSt). *Vice versa* the public prosecutor and the criminal court are obliged to inform the bar lawyer of an investigation against a lawyer or a trainee lawyer and to send him a copy of the final decision of the case. In cases

where a lawyer also commits (a) criminal offense(s), like for example ML or FT, he/she is not only subject to disciplinary supervision and sanctions but also to criminal penalties. The criminal sanctions include effective, proportionate and dissuasive sanctions with regards to persons that fail to comply with national AML/CFT requirements. Criminal proceedings are of the competence of the criminal courts in Austria. All in all lawyers have to face additional sanctions besides the ones according to the StGB (up to the removal from the list of lawyers, which will mean the loss of the means of existence in many cases, in addition to criminal sanctions). Disciplinary sanctions have been pronounced based on the AML provisions of the RAO, including deletions from the list of lawyers.

### **Civil Law Notaries**

972. The competent regional Chamber of Civil Law Notaries (SRO) is obliged to examine the files of notaries within its remit to review their business activities from time to time. This includes verifying whether notaries comply with the provisions preventing or fighting ML or FT. Dedicated teams of examiners review the activity of all notaries, including AML/CFT requirements, on a three year basis. Random controls are also performed on about 10 percent of the notaries every year. A report is sent to the board of the Chamber. In the case of deficiencies a reminder is sent to the notary in order to receive a clarification.

973. If the regional Chamber of Civil Law Notaries detects facts related to ML or FT, it must report its suspicion to the BKA (cf. Article 154 NO). If a notary violates a statutory obligation in the context of AML/CFT (imposed e.g., by the NO), he/she is in breach of a professional duty that will be sanctioned as a major disciplinary offense by the higher regional court as the disciplinary court after a hearing by the senior public prosecutor, or as a minor disciplinary offense by the competent regional Chamber of Civil Law Notaries (cf. Article 155 NO). Concerning the general activity of monitoring, 16 cases were passed to the higher regional court during the period 2005–2008, and 5 notaries were convicted. One of these cases was ML-related, in 2008.

974. The scale of sanctions for major offenses ranges from a written reprimand or a fine of up to EUR 36,000 to suspension from office for up to one year or to debarring from office. Sanctions for minor offenses include cautioning on the professional duties, admonition in writing or admonition in writing in combination with a fine of up to EUR 7,200 (cf. Article 158 NO).

### **Chartered Public Accountants and Tax Consultants**

975. The Chamber of Chartered Public Accountants and Tax Consultants has no specific powers to monitor and ensure compliance of chartered public accountants and tax consultants with AML/CFT requirements. It has no power to apply effective, proportionate and dissuasive sanctions to these professions.

### **Accountancy Professions**

976. The Parity Commission for the Accountancy Professions has no specific powers to monitor and ensure compliance of the accountancy professions with AML/CFT requirements. It has no power to apply effective, proportionate and dissuasive sanctions to these professions.

### ***Guidelines for DNFBPs (c. 25.1)***

## **Casinos**

977. Guidance is currently contained in the “AML/CFT Safety Measures” of casinos, issued by the licensee itself in cooperation with the MoF in 2007 and updated on October 8, 2008 to take into account the amendments to the GSpG. This guidance is enforceable by the MoF pursuant to Articles 19 and 31 GSpG. According to Article 25a GSpG, as well as by reference of Article 25, paragraph 6 GSpG to Article 41, paragraph 2 last two sentences BWG, the MoI is responsible for guidance to casinos. But no tailored guidance has been issued.

## **Real Estate Agents, Dealers, Management Consultants and Insurance Intermediaries**

978. According to Article 365z, paragraph 4 GewO the MoI is obliged to inform tradespersons by way of the professional chambers about methods of ML and FT and any hints on suspicious transactions. There is currently no specific guidelines established by the A-FIU, the MoE, or the WKO. Some guidance can be found in the explanatory notes to the amendments to the GewO, but it is not an easy tool to be used by the tradespersons.

## **Lawyers**

979. Guidance is currently prepared by the Bar Association in cooperation with the MoJ, but has not yet been finalized.

## **Civil Law Notaries**

980. The Austrian Chamber of Civil Law Notaries has compiled a non-binding guidance for Austrian notaries to prevent ML and FT, updated in April 2008.

## **Chartered Public Accountants, Tax Consultants and Accountancy Professions**

981. The MoE, the Chamber or the Parity commission have not issued guidance for accountants.

## ***Feedback to DNFBPs (c.25.2)***

982. General feedback can be found in the A-FIU Annual report but is limited due to the limited number of STRs received from DNFBPs. From the meetings with the business and professions there is no evidence of a systematic case by case feedback.

983. Concerning casinos, the MoI has to make sure, as far as this is practicable, that the licensee receives a feedback in due time regarding the effectiveness of notices of suspicion according to Article 25(6) and (7) and of the measures taken as a consequence. The new version of Article 25a was enacted in July 2008, and it was not possible at the time of the assessment to assess the implementation of this new requirement. In the past, few exchanges seem to have taken place between the A-FIU and casinos, but without systematic feedback on STRs.

984. Concerning professions regulated by the GewO, two presentations with representatives from the MoE and from the MoI, in June 2003 and in October 2007, took place in Carinthia. Besides this and some information in the annual report of the A-FIU concerning statistics of STRs by DNFBPs, the feedback to the tradespersons, either general or specific, is still at an early stage.

### 4.3.2 Recommendations and Comments

985. The authorities should:

#### Recommendation 24

- Give the Ministry of Finance adequate powers to perform AML/CFT supervision of internet casinos;
- Empower the Ministry of Finance to perform controls on the beneficial owners of a significant or controlling interest in casinos, and to prevent actions by associates of criminals;
- Put in place a system for monitoring and ensuring compliance with AML/CFT requirements to cover accountants and all the companies active in the TCSP sector;
- Give trade authorities the necessary technical and budgetary resources to perform effectively their functions;
- Review the amount of the fines permissible under the GewO.

#### Recommendation 25

- Establish guidelines tailored to the specific needs of each DNFBP, as these currently exist only for notaries, and partially for casinos;
- Provide information on current techniques, methods and trend tailored to each DNFBP, as well as systematic case by case feedback on STRs.

### 4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
<b>R.24</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Absence of adequate powers to perform supervision of internet casinos.</li> <li>• Absence of power to control the beneficial owners of a significant or controlling interest in casinos, and to prevent actions by associates of criminals.</li> <li>• Absence of systems for monitoring and ensuring compliance with AML/CFT requirements for accountants and all the companies active in the TCSP sector.</li> <li>• Lack of effectiveness and resources to implement the measures envisaged by the GewO.</li> <li>• Inadequate sanctioning powers.</li> </ul>
<b>R.25</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Absence of guidelines for all DNFBPs but notaries and casinos.</li> <li>• Limited general feedback tailored to the specific needs of each DNFBPs,</li> </ul>

		and absence of systematic case by case feedback on STRs.
--	--	--

#### **4.4 Other Non-Financial Businesses and Professions—Modern-Secure Transaction Techniques (R.20)**

##### **4.4.1 Description and Analysis**

###### ***Other Vulnerable DNFBPs (c. 20.1)***

986. As mentioned above, the GewO goes beyond the 40+9 Recommendations as far as dealers are concerned: not only dealers in precious stones and metals are subject to the regulations in the GewO but all dealers and auctioneers when doing cash transactions above EUR 15,000. Additionally, AML/CFT requirements apply to all accountants regardless of the business activity they are involved in (see Chapter 4.2, c. 16.5).

987. It has to be noted that the inclusion of those other businesses and professions has not been decided on the basis of a specific risk analysis in Austria. On the contrary, the authorities consider that the professions covered by the GewO present a low ML/FT risk. But Austria took part in the EU decision to apply AML/CFT measures on all dealers.

###### ***Modernization of Conduct of Financial Transactions (c. 20.2)***

988. The authorities developed the initiative “e-payments in the public administration” that promotes the idea of cashless payment by accepting debit and credit card payments in all public departments and offices/government agencies. In 2007, these transactions amounted to approximately EUR 143 million. In addition, cash payments by Federal authorities to citizens are reduced systematically.

989. The issue of the modernization of the conduct of financial transactions is of particular interest in Austria where the authorities acknowledge that cash is relatively more used than in other similar European countries. The importance of cash used in internal and external relations is also noticeable in the statistics provided by the customs on the declaration by cash couriers estimated to an average of EUR 1 billion each quarter. In addition, an interesting statistic is the evolution of the net number of 500 Euro banknotes issued by the OeNB (Banknotes issued–Banknotes withdrawn), that increased by more than 250 percent between July 2007 and July 2008. The authorities indicated that certainly not all these 500 Euro banknotes have been disseminated in Austria. The assessors were also informed that some Austrian banks are active in the business of foreign exchange cash clearing for financial institutions in countries of Eastern and South-Eastern Europe. In addition, the authorities explained that countries bordering the Euro Area, like Austria, take care of the demand for Euro banknotes in the neighboring non-Euro area countries where Euro is used as a parallel currency, and that the OeNB took care of the initial demand for Euro banknotes in Slovenia and Slovakia. For example, Slovenia introduced the Euro in 2008, which is considered as a reason why the number of banknotes issued increased after July 2007.

990. The authorities have not provided information on the measures they are taking to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to ML, except for transactions with the public administration. For example, no

specific measures related to AML/CFT have been taken in the context of the currency changeover of the neighboring countries of Slovenia (January 2008) or Slovakia (January 2007). No comprehensive analysis of the AML/CFT risks related to currency exchange and cash couriers has been conducted and the supervision of the banks active in the currency exchange appears currently limited.

#### 4.4.2 Recommendations and Comments

991. The authorities should conduct a domestic analysis in order to determine the risk for dealers, other than dealers in precious metals and stones, of being misused for ML or FT. They should also consider whether other non-financial businesses and professions are at risk of being misused for ML or FT.

992. The authorities should:

- take additional measures to reduce the relative importance of use of cash and large denomination banknotes.

#### 4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	LC	<ul style="list-style-type: none"> <li>• Insufficient measures to reduce the relative importance of use of cash and large denomination banknotes.</li> </ul>

## 5. LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANIZATIONS

### 5.1 Legal Persons—Access to Beneficial Ownership and Control Information (R.33)

#### 5.1.1 Description and Analysis

##### Legal Framework

993. The Austrian Law recognizes the following types of legal persons:

- Limited liability company;
- Joint-stock company;
- European Society;
- Cooperative society;
- European cooperative;
- Association; and
- Private foundation.

994. Legal persons come into legal existence by registration in the Commercial Register, which is maintained at the courts of first instance on commercial matters (*Firmenbuchgericht*). The

Commercial Register is accessible online to the public via special websites authorized by the MoJ with a small fee. The Commercial Register is administered at Regional Court level. There are a total of 16 courts dealing with matters of the Commercial Register.

995. Newly formed corporations must record their articles of incorporation and submit the application signed by all founders, members of the supervisory board and the board of management to the court responsible for the Commercial Register. When the court decides that all statutory requirements have been complied with, it will order the registration and publication in the official gazette (“*Amtsblatt zur Wiener Zeitung*”) and through the Internet (Ediktsdatei, available via [www.edikte.justiz.gv.at](http://www.edikte.justiz.gv.at)).

996. Associations have to be registered with the relevant “*Vereinsbehörde*” (local district authority or Federal Police Directorate), which can refuse the registration if the association or its purpose infringe Austrian law. Each association is registered under a “register number” and listed in the Central Register of Associations (ZVR). The ZVR is a public register, kept by the MoI and accessible online by anyone (<http://zvr.bmi.gv.at/Start>).

997. Foreign corporations can establish branch offices in Austria, which, before starting business activities, must be entered in the Commercial Register at the commercial court competent for the district in which the branch has its seat. In this case, the disclosure requirements set forth in the case of companies incorporated under Austrian law will be applied analogically, based on the type of mother company in the incorporating jurisdiction.

#### **Limited Liability Company (*Gesellschaft Mit Beschränkter Haftung, Ges.M.B.H.*)**

998. A limited liability company is formed under the Austrian Limited Liability Companies Act (*GmbHG*). The shareholders' liability is limited to the unpaid portion of the par value of the shares. Authorities indicate (but no precise figures where provided) that most of the foreign owned businesses in Austria operate in this legal form. The minimum capital is EUR 35,000.

999. The company acts through its directors; a supervisory board is obligatory, if either the subscribed capital exceeds EUR 70,000 and the number of shareholders exceeds 50 or there are more than 300 employees. A notarial deed is required for its formation.

1000. Private limited liability companies must register with the regional court of first instance in commercial matters. The application must be accompanied by the company's statutes authenticated by a public notary, a list of shareholders, a list of the appointed managers, an affidavit from the managers that the minimum capital required will be retained, specimen signatures of managers and confirmation by the tax authorities that the capital transaction tax has been paid or guaranteed.

1001. The identity (name, date of birth) of the directors (and members of the supervisory board, when obligatory) as well as of shareholders (natural or legal persons, name and date of birth respectively registration number) is disclosed and maintained at the Commercial Register. Every change to a shareholder's identity must be registered in the Commercial Register. Shareholders who are not registered in the Commercial Register are precluded from exercising any of their rights vis-à-vis the company. In addition, non-compliance with registration requirements is punishable by fine.

1002. As of December 1, 2007 there were 110,997 limited liability companies listed in the Commercial Register.

**Joint-Stock Company (*Aktiengesellschaft, AG*)**

1003. The Joint-stock company is a stock corporation established under the Stock Corporation Act (*Aktiengesetz, AktG*). The incorporators subscribe for the shares and sign the articles of incorporation. The articles must state the corporation's name, its purpose, the nominal amount of share capital, number and par value of each class of shares, the composition of the board of management and the form in which its notices will be published. The minimum capital stock is EUR 70,000. A supervisory board is obligatory; a general meeting of shareholders ("*Hauptversammlung*") must be held annually.

1004. For the formation of a joint-stock company a notarial deed is required. Joint Stock Companies are also required to register with the regional court of first instance in commercial matters. The application must be accompanied by the company's statutes authenticated by a public notary, a list of shareholders, a list of the appointed managers, an affidavit from the managers that the minimum capital required will be retained, specimen signatures of managers and confirmation by the tax authorities that the capital transaction tax has been paid or guaranteed.

1005. The identity (name, date of birth) of the directors and members of the supervisory board is maintained in the Commercial Register.

1006. The Joint-stock company can issue nominative or bearer shares (in the latter case also up to the 100 percent of the capital). If the company is listed in the Stock exchange it will also have to comply with the provisions set forth by the BörseG. Bearer shares can be traded in the Stock Exchange. The authorities informed that in the Stock Exchange shares are only traded in a bearer form, although they indicate that, based on practice, the shares are "de facto" de-materialized.

1007. If there is only one shareholder, irrespective whether the shares are nominative or in bearer forms, his/her name (natural or legal person) is also maintained in the Commercial Register. In the case in which there are more shareholders, their names are not maintained by the Commercial Register, irrespective of whether the company has issued bearer shares or nominative shares. In case of a company with nominative shares, the shareholders' register is kept by the company and is open to inspection to any shareholder. According to § 61 AktG the owners of nominative shares (and provisional certificates, which are issued, also in the case of bearer shares, in the case the capital has not been entirely paid up) have to be registered in a shareholders' register maintained by the company. Thus, the transfer of nominative shares (and provisional certificates) has to be notified to the company, the shares have to be submitted and the transfer has to be verified. On the basis of this evidence, the transfer of the shares is registered in the shareholders' register. Vis-à-vis the company only registered shareholders are considered as shareholders: shareholders whose names are not entered in the shareholders' register (in the case in which registered shares were issued) are precluded from exercising any of their rights vis-à-vis the company.

1008. As of December 1, 2007 there were 2,057 Joint-stock companies listed in the Commercial Register.

**European Company (*Europäische Gesellschaft – Societas Europaea, Se*)**

1009. The European Company is regulated by Council Regulation (EEC) no. 2157/2001 of 8 October 2001 on the Statute for a European Company and the Austrian Societas Europaea Act (*Societas Europaea-Gesetz, SEG*).

1010. The registration and disclosure requirement of a European Company are the same of a joint stock company.

1011. As of December 1, 2007, there were 10 European Companies registered in the Commercial Register.

**Cooperative Society (*Erwerbs- Und Wirtschaftsgenossenschaft*)**

1012. The cooperative society is a corporation without a fixed number of members. The purpose of a cooperative is to assist its members. A cooperative can be established either with a limited (which is the rule) or unlimited liability (which is rare).

1013. Cooperative societies are registered in the Commercial Register, but no information about members' or their identities is disclosed in the Commercial Register. However, the cooperative society itself is required to keep a register of its members and make it available for inspection to anyone who requires to see it. This register contains also the list of the managers and, if applicable, the members of the supervisory board.

1014. As of December 1, 2007, there were 1,900 cooperative societies registered in the Commercial Register.

**European Cooperative Society (*Europäische Genossenschaft - Societas Cooperativa Europea, SCE*)**

1015. A European Cooperative Society is regulated by Council Regulation (EEC) no. 1435/2003 of 22 July 2003 on the Statute for a European Cooperative Society (SCE) and the Austrian Societas Cooperativa Europaea Act (*Societas Cooperativa Europaea-Gesetz, SCEG*). The Regulation stipulates that the activities of the cooperative should be conducted for the mutual benefit of the members so that each member benefits from the activities of the SCE in accordance with his/her participation, and members of the SCE should also be customers, employees or suppliers or should otherwise be involved in the activities of the SCE. Rights of control should be vested equally in members, although weighted voting may be allowed in order to reflect each member's contribution to the SCE.

1016. A European Cooperative Society may be established by at least five natural persons and/or companies in different Member States, by a merger between cooperatives of different Member States or by conversion of a cooperative, if it has had an establishment or subsidiary governed by the law of another Member State for at least two years. The subscribed capital must not be less than EUR 30,000. The registration and disclosure requirements are the same as those of a Cooperative Society (Article 5a Commercial Register Act, *Firmenbuchgesetz, FBG*). The statutes have to contain also the list of the members which founded the SCE (Article 5, paragraph 4 SCE-Reg). As the Cooperative Society, the SCE is required to maintain a register of its members (Article 14, paragraph 4 SCE-Reg).

1017. As of December 1, 2007, there was no European Cooperative Society listed in the Commercial Register.

### **Association (*Verein*)**

1018. An association is a voluntary, permanent organization which consists of at least two persons and is established based on statutes with the aim of achieving a specific common objective. An association must not be profit-oriented and may use its assets only in the interest of promoting its objective. In Austria, most NPOs take the form of associations (*Vereine*).

1019. Associations have legal personality and are regulated by the Associations Act (*Vereinsgesetz, VerG*). The VerG, however, does not apply to types of associations which, pursuant to other legal regulations, must be established as other legal forms or which, as a result of free choice of legal form, are established pursuant to other legal regulations.

1020. Associations are governed by statutes. These statutes must contain information inter alia on the name and seat of the association (exclusively in Austria), its purpose, intended activities and means of covering financial needs, membership and other organizational information.

1021. The supreme decision-making body of an association is the general meeting of all members, which has to be convened at least every four years. Moreover, every association must be headed by a governing body which is appointed to manage its affairs and to represent the association in public. This governing body has to consist of at least two persons (according to the principle of “two pairs of eyes”/dual control).

1022. Once a year, the financial management of an association must be examined by at least two auditors (*Rechnungsprüfer*) who are to be appointed by the association and who must be independent and impartial. Instead of two auditors, large associations must appoint a statutory auditor (*Abschlussprüfer*) who must also be independent and impartial. Statutory auditors may be certified auditors and tax consultants or auditing and tax consultancy companies, chartered accountants and tax consultants or accounting and tax consultancy companies.

1023. The foundation of an association requires two steps: it is established through the agreement of statutes (Deed of Establishment), but the association does not attain legal capacity until the expiry of a four-week period after the declaration of establishment is received by the competent association authority or until an earlier affirmative decision issued by the association authority. If a first inspection of the submitted statutes raises the responsible association authority’s suspicion that the objective, name or organization of an association might be illegal, the association authority is entitled to extend this four-week period to a maximum of six weeks by means of an official notification, should this be necessary for a proper investigation of the issues in question. Under certain legal circumstances, the association authority may refuse to authorize the foundation of an association. Under certain legal circumstances, the association authority is also entitled to dissolve an association.

1024. All associations are listed in a public register (ZVR). Unless a non-disclosure right was granted because of association interests worth being protected, everyone is entitled to retrieve specific data on an association (e.g., regulation of the association’s representation as per statutes or the names of the association organ’s representatives) through free individual online queries if the association in

question is unambiguously identifiable based on its number in the Central Register of Associations or its name or parts of its name, combined—if necessary—with its registered office.

1025. As of December 31, 2007, there were 111,282 associations listed in the Central Register of Associations.

### **Private Foundation (*Privatstiftung*)**

1026. Private foundations are regulated by the Law on private foundations (*Privatstiftungsgesetz, PStG*). A private foundation is a legal entity set up by a declaration of establishment, which must be filed with the Commercial Register. The declaration of establishment documents the legal intent of the founder (the grantor, who may be one or several individuals or legal persons) to dedicate assets for a specific purpose, determined by the founder. The minimum amount of assets to be donated to the private foundation is EUR 70,000, which may be contributed in cash (certified by a bank) or in kinds or other assets.

1027. The private foundation can be established not only with an act *mortis causa* but also *inter vivos* and may not only have purposes of charitable or public benefit, but also serve a merely personal interest (for example regular payments to the grantor's family members; the grantor can be the beneficiary of the foundation); however there is a strict prohibition on engaging in commercial activities (only activities that are necessarily connected with the original trusteeship are allowed), but the private foundation can participate in a limited partnership or even in the "silent" partnerships.

1028. The founding deed, which must be authenticated by a public notary, must indicate the name of the founder/grantor, the scope of the foundation, the names of the members of the board of trustees (who represent the private foundation) and the names of the members of the supervisory board (when such board is required). The founding deed is maintained by the Commercial Register.

1029. The beneficiaries of the foundation can be also nominated in the founding deed (in which case their names will be accessible at the Commercial Register); however the beneficiaries can also only be nominated in an appendix or supplementary declaration to the founding deed, which is not subject to registration at the Commercial Register, nor otherwise accessible. In the case in which the beneficiary receives a payment or other economic benefit from the foundation, this will have to be declared to the tax authorities. Therefore, only in this situation, when the appendix had not been registered, will the beneficiary's identity be known to the tax authorities.

1030. There are no limitations for non residents to set up private foundations or for being the beneficiaries of a foundation.

1031. The main reason for establishing a private foundation is to benefit from tax incentives, such as a flat rate of 2,5 percent inheritance or donation tax whenever the foundation is endowed with assets by its grantor (also in cases of subsequent endowments after the foundation) or a flat tax of 12,5 percent on corporate income tax. However the inheritance/donation tax has been recently levied for anyone, making the foundation less attractive from this standpoint. However, one of the major advantages of setting up a private foundation, as acknowledged by the authorities, is the fact that beneficial ownership (that is the beneficiaries, as the foundation does not have an owner but "own itself") can be easily hidden, for example when the names of the beneficiaries are only indicated in the appendix to the founding deed. Private foundations may also be used to circumvent the strict

limitations to purchase real estate set forth by the Land Control Act for foreigners who are not EC citizens.

1032. As of December 1, 2007, there were 3,028 private foundations listed in the Commercial Register.

***Measures to Prevent Unlawful Use of Legal Persons (c. 33.1)***

1033. Austria mainly relies on a system of central registration that – but only to a limited extent – allows for transparency concerning the beneficial ownership and control of legal persons. For all types of legal persons, the laws require that the name and date of birth of the founders, the original shareholders, and managers and directors, as well as the company’s statute or the private foundation deed of establishment are registered with the Commercial Register. This information is available to anyone, on line, for a small fee, so access to it is timely.

1034. Any subsequent changes to a shareholder’s identity must be registered in the Commercial Register, under penalty of a fine, but only with respect to limited liability companies (in all instances) and joint stock companies (only for the case of joint stock companies with a single shareholder). There is no requirement to register changes in the ownership of shareholders for joint stock companies with more than one shareholder (or in the case of owners of bearer shares) nor for European companies. The only change that would be subject to registration, in these instances, is if the joint stock company (or the European company) from a multi-shareholders proprietorship becomes owned by a single shareholder (which is subject to immediate registration in the Commercial Register).

1035. In these instances, Austria relies on the investigative powers of its law enforcement authorities, particularly the power to search places, objects and persons set forth by Article 119 of the StPO. This provision allows the search of places (premises that are not publicly accessible) if, due to ascertained facts, it can be assumed that there are objects that have to be seized or examined. The search can be conducted by the criminal police at their own discretion (and then reported as soon as possible to the office of the public prosecutor).

1036. There are instances however—such as in the case of a holder of bearer shares who does not exercise the right of vote at the general meeting or, in the case of a private foundation, a beneficiary whose name is only in the appendix/supplementary declaration of the founding deed—in which the exercise of such investigative powers are not sufficient *per se* to ascertain the company’s real beneficial ownership, nor to obtain the information on the beneficial owner in a timely fashion. The authorities indicated that the majority of companies registered in Austria are limited liability companies and almost 25 percent of the joint-stock companies registered in Austria only have one shareholder.

***Access to Information on Beneficial Owners of Legal Persons (c. 33.2)***

1037. In the case of joint stock company the capital of which is represented by nominative shares, registration of the change of ownerships in the Commercial Register is only required in the case of a single shareholder. In the case of multiple shareholders, the change in ownership is only mentioned in the shareholder register that is kept by the company and is open to inspection by any shareholder.

Law enforcement authorities can have access to the shareholders' register under Article 119 of the StPO.

1038. If the shares are issued in bearer form, it is difficult to ascertain beneficial ownership. The name of the bearer of the shares (who may not be the real beneficial owner) will only be registered if the holder of the bearer shares wants to exercise the right of vote at the general meeting of the company. According to Article 110 AktG, all shareholders and their representatives who participate in the general meeting have to be registered in a list of participants which has to be added to the minutes of the general meeting and registered at the Commercial Register. This includes the holder of bearer shares.

1039. With respect to private foundation, when the name of the beneficiary is only in the appendix/supplementary declaration of the founding deed (which is not subject to registration with the Commercial Register), such information may be available only to the tax authorities, but only in the case of payments/receiving of economic benefits subject to tax declaration. These limited circumstances substantially hinder the access to the information in a timely fashion. A search of premises or person—which could be undertaken by the Police—would not be conclusive *per se*.

***Prevention of Misuse of Bearer Shares (c. 33.3)***

1040. As mentioned above, in the case of a joint stock company with multiple shareholders, the capital of the company can be represented up to its entirety by bearer shares. The law requires that the holder of a bearer share be registered if he/she wants to exercise the right of vote at the company's general meeting. However, other than in this circumstance, there is no possibility to ascertain beneficial ownership of the bearer shares, which may pose a risk of ML and FT. The authorities explained that, according to Article 10 AktG, the shares (even in bearer form) must be registered if issued before full payment of the issuing price. Before full payment only provisional certificates (*Zwischenscheine*) can be issued which have to be registered in the shareholders' register maintained by the company like nominative shares (Article 61, paragraph 6 AktG).

1041. It has to be noted that, in practice, in the Austrian Stock Exchange, the majority of the shares traded are only in bearer form. Authorities explained that, in practice, the bearer shares traded in the Stock Exchange are “de facto” dematerialized. No written individual certificates are issued, and the shares can in practice only be held and traded through banks who hold the (virtual) shares in their deposit. Authorities also explained that in the case of capital market-orientated joint-stock companies, in practice, a global certificate is handed to the Central Securities Depository (CSD, i.e., the Oesterreichische Kontrollbank) Authorities maintain that since opening a securities account at a financial institution means entering a business relationship with the respective financial institution the account holder has to be identified and his identity to be verified. Thus, in this case, investigators can trace the ownership via the chain of book-entries, beginning with the CSD right to the shareholder. In the case of noncapital market-oriented joint-stock-companies (mostly family companies), authorities maintain that the practice is not to issue shares, but certificates. In this case, the owners of the certificates have to be entered in a register maintained by the company.

1042. The authorities also reckon that joint stock companies whose capital is in the form of bearer shares are not suitable for being misused as vehicles for criminal activities, as the costs of the establishment, management and the winding up would be too high for these—typically only

transient—purposes. Authorities also point out that of the 2,057 joint-stock companies registered in Austria, 426 have only one owner (in which case information on the beneficial owner will be available directly in the Commercial Register), and another 116 companies are listed, which means their shares are de facto dematerialized. This means that some 1,500 joint stock companies (as of December 2007) may choose or may have chosen to issue shares in bearer form or in a registered form.

1043. However, these figures are not conclusive, as they do not indicate the exact percentage and the value of bearer shares that have been issued (which would be useful for the analysis of the ML risk). It would appear that the volumes of bearer shares may be high, as historically the issuing of bearer shares has been particularly common for companies owned or controlled by large wealthy families, as a way to facilitate transfers of shares among family members. Also, in the Stock Exchange only shares in bearer forms are traded, and the fact that the de-materialization is only a practice may not exclude situations of risk of ML.

1044. The authorities also pointed out that because of the requirement that the bearer shares be forgery-proof (or for practical reasons, for example to prevent that the shares are sold to a non-family member), they are usually accompanied by a certificate that indicate the name of the owner.

1045. No risk assessment appears to have been undertaken by the authorities to ascertain the risk of ML/FT in joint stock companies which have issued bearer shares, nor in foundations, where the founding deed does not indicate the name of the beneficiaries. In these instances these legal persons do not provide for a transparent structure of the beneficial ownership, and can be used as vehicles to launder money or for FT.

***Additional Element—Access to Information on Beneficial Owners of Legal Persons by Financial Institutions (c. 33.4)***

1046. Financial institutions can have direct access to beneficial owners' information only for the information available in the Commercial Register.

**5.1.2 Recommendations and Comments**

1047. The authorities should:

- Make the regime of private foundations more transparent on beneficial ownership, for example by requiring that the appendix/supplementary declaration be available in the Commercial Register, to reduce the risk that these foundations may be used for ML;
- Establish a legal mechanism to trade shares in the Stock exchange in nominative form or adopt legal provisions to make “de-materialization” mandatory;
- Conduct an assessment to determine the ML risk potentially associated to the use of bearer shares.

### 5.1.3 Compliance with Recommendation 33

	Rating	Summary of factors underlying rating
R.33	PC	<ul style="list-style-type: none"> <li>• Insufficient capacity to ascertain beneficial ownership in the case of companies that issue bearer shares and, in some instances, in the case of private foundations.</li> <li>• Competent authorities not always able to obtain or access to adequate, accurate and current information on the beneficial ownership and control of legal persons in a timely fashion.</li> <li>• No risk assessment undertaken by the authorities to ascertain the risk of ML/FT in the case of joint stock companies which have issued bearer shares, nor in the case of foundations, where the founding deed does not indicate the name of the beneficiaries.</li> </ul>

## 5.2 Legal Arrangements—Access to Beneficial Ownership and Control Information (R.34)

### 5.2.1 Description and Analysis

#### Legal Framework

1048. Common law trusts cannot be set up under Austrian law. However, trustees can act from within Austria with respect to trusts established under other countries' laws. A foreign trust may therefore have all or part of its administration in Austria—for example records, banking arrangements, assets. No information was provided as to the number of foreign trusts administered in Austria and the amounts that they represent.

1049. Austria has other legal arrangements, namely the foundation (*Stiftung*) and the *Treuhand*. The fideicomiso however does not exist under Austrian law.

1050. The Austrian foundation is a legal person and is therefore dealt with under Recommendation 33 above.

1051. The *Treuhand* is a civil contract which is not regulated in law, but is based on the general principle of the autonomy of the contracting parties and delimited by jurisprudence and doctrine. It is created when a person, the *Treuhänder*, is authorized to exercise rights over property in his or her own name, on the basis of and in accordance with a binding agreement with another person, the *Treugeber*. There are two main types of *Treuhand*, the *Fiducia* and the *Ermächtigungstreuhand*. With the *Fiducia* most of the rights are transferred to the *Treuhänder*, whereas the *Ermächtigungstreuhand* only entails a transfer of certain rights such as the right to manage the assets. The *Treuhand* can exist without any written record. It can be concluded between any two persons capable of being party to a contract. The *Treugeber* and the *Treuhänder* may chose to inform third parties of the legal arrangement between them (*offene Treuhand* or open *Treuhand*) or not (*verdeckte Treuhand* or hidden *Treuhand*).

1052. The Austrian *Treuhand* entails a form of split ownership: the *Treuhänder* is the legal owner of the assets but the *Treugeber* maintains the “economic ownership” and may therefore claim compensation for his or her property in certain circumstances, such as the *Treuhänder*’s bankruptcy. The *Treuhänder* has all the rights linked to the property in relation to third parties, but may be held liable towards the *Treugeber* in case of breach of the *Treuhand* agreement. Only the *Treuhänder* is entitled *in rem* to the property whereas, in principle, the *Treugeber*’s rights are restricted to personal claims against the *Treuhänder*.

1053. Although no precise figures exist on the subject, the Austrian *Treuhand* is a very common feature of the Austrian economy. Lawyers, notaries and other TSP often act as *Treuhänder* but any member of the general public who can be party to a contract can act as *Treuhänder*.

***Measures to Prevent Unlawful Use of Legal Arrangements (c. 34.1)***

1054. As far as foreign trusts are concerned, there are no measures in place to ensure transparency other than the customer due diligence requirements applicable where the trustee is a financial institution or a DNFBP described earlier in this report. There is, for instance, no registration of foreign trusts or of trustees: while lawyers, notaries, accountants, management consultants and others are able to conduct trust service business and “act or arrange to act as a trustee of an express trust or other similar arrangement”, there is no register that would list foreign trusts that are operated from Austria.

1055. As far as the Austrian *Treuhand* is concerned, there is a partial registration system in place, in the sense that some form of registration is required depending on the profession of the *Treuhänder* the nature of the property, and, in the case of funds, their amount:

- Lawyers and notaries acting as *Treuhänder* are subject to the AML/CFT measures described above, as well as those set out in Article 8a ff RAO and Article 9b RL-BA for lawyers, and in Article 36a ff and 109a and in the guideline THR 1999 for notaries;
- According to the Bar Associations’ Guidelines, lawyers must register every *Treuhand* of more than EUR 15,000 or EUR 40,000 (depending on the federal state legislation) at the Register of Escrows of the competent Bar Association (*Treuhandbuch*);
- Pursuant to the THR 1999, notaries should register every *Treuhand* of more than EUR 10,000 in the digital Register of Escrows maintained by the Austrian Chamber of Civil-Law Notaries.

1056. However, both rules above only apply to funds, and not to other types of property, and are only applicable to lawyers and notaries. There are no measures in place for other *Treuhänders*. It is therefore impossible to determine how many *Treuhand* are established, the amount of property that they cover, and who the *Treuhänders* are.

1057. Although police investigation powers in criminal matters are good, because there is neither a central register of *Treuhand*s, nor a register of persons authorized to act as a *Treuhänder*, a police investigator seeking information would have to check with each and every relevant professional before locating the *Treuhänder* he/she is looking for. If the *Treuhänder* is not a member of the Bar Association or is not a notary, the search is virtually impossible. Additionally, the various bodies currently charged with the oversight of the TSPs have little ability to share information between one

another or to extend international assistance to foreign counterparts. The only available channel for information sharing is Article 22 B-VG (“*Amtshilfe*”).

1058. Another channel of information may be provided to a certain extent by the banking provisions. Pursuant to the BWG, where a fiduciary relationship exists, it must be brought to the attention of the bank when opening an account. Although useful this provision is only partially helpful in reducing the likelihood of the unlawful use of legal arrangements for ML or FT purposes, because it only addresses circumstances where the assets are placed in a bank account. It does not address the AML/CFT risks as satisfactorily as effective oversight of trust and corporate services providers, as the *Treuhand* may not need access to an Austrian bank account, the *Treuhänder* choosing perhaps an account in a jurisdiction without the provisions of the BWG outlined below, or because the *Treuhänder* simply arranges for assets to be settled directly into the *Treuhand* without going through the bank transaction stage at all. For example, assets such as shares, real estate or high value goods can be settled into the *Treuhand* by assignment, achieving the objective of laundering money while by-passing the legislative controls in place which relate to bank accounts only. (Whereas the AML/CFT defenses of a properly conducted TSP would involve recording all assets, where they came from, their value, location, etc). Furthermore, the burden placed on the authorities to lift the banking secrecy requirements that are described under previous recommendations would also apply in this case.

1059. In brief, while access to the investigation power is available in a timely fashion, its effectiveness is undermined in the practical difficulty in knowing where to turn enquiries in the absence of registers or consistent Trust Service Provider (TSP) sector oversight and the strict conditions for lifting banking secrecy.

***Access to Information on Beneficial Owners of Legal Arrangements (c. 34.2)***

1060. As mentioned above, there are no measures in place to ensure access to beneficial ownership information on foreign trusts that are dealt with in Austria.

1061. As for the Austrian *Treuhand*, the situation is very much the same as described above: access to beneficial ownership information is only available in a limited number of circumstances.

***Access to Information on Beneficial Owners of Legal Arrangements by Financial Institutions (c. 34.3)***

1062. The BWG is helpful with regard to improving a financial or credit institution’s access to information on beneficial owners of legal arrangements in three important respects. Firstly, Article 40,(2) of the BWG requires credit or financial institutions to ask the customers whether they intend to conduct the business relationship or transaction on behalf of a third party; second, where customers confirm they do so intend, the law places an obligation on them to disclose the name of the trustor (or *Treugeber*) to the institution and for trustor’s identity to be established; third, Article 41(1)2 applies an obligation on the financial or credit institution to make a suspicious transaction report if the institution suspects that the customer has violated his obligation to disclose a fiduciary relationship and finally the law makes it an offense for the person acting as a trustee to fail to disclose this to the credit or financial institution.

1063. These are helpful provisions, in that they facilitate access to control information required by financial institutions, both in respect of the Austrian *Treuhand* and for customers that are acting in a fiduciary capacity for arrangements deriving from other countries. Despite these important characteristics the importance of effective oversight of the trust and company service providers for the purposes of AML/CFT should not be overlooked and is dealt with in other sections of this report.

### 5.2.2 Recommendations and Comments

1064. The authorities should:

- Ensure transparency where the property held in *Treuhand* is composed of assets other than funds (regardless of the *Treuhänder*), where the *Treuhänder* is someone other than a lawyer, notary or registered TSP, where funds held under *Treuhand* by lawyers amount to less than the federal state threshold (i.e., between EUR 15,000 and EUR 40,000);
- Ensure transparency over foreign trusts operated from Austria;
- Implement AML/CFT oversight to ensure TSPs properly obtain, verify and record details of the *Treuhand* and its beneficial ownership;
- Develop effective means by which bodies charged with the oversight of TSPs for AML/CFT purposes can share information with their national or foreign counterparts.

### 5.2.3 Compliance with Recommendation 34

	Rating	Summary of factors underlying rating
R.34	PC	<ul style="list-style-type: none"> <li>• No transparency where the property held in <i>Treuhand</i> is composed of assets other than funds (regardless of the <i>Treuhänder</i>); where the <i>Treuhänder</i> is someone other than a lawyer, notary or registered TSP; where funds held under <i>Treuhand</i> by lawyers amount to less than the federal state threshold (i.e., between EUR 15,000 and EUR 40,000).</li> <li>• No transparency over foreign trusts operated from Austria.</li> <li>• No effective AML/CFT oversight to ensure TSPs properly obtain, verify and record details of the <i>Treuhand</i> and its beneficial ownership.</li> <li>• No effective means by which bodies charged with the oversight of TSPs for AML/CFT purposes can share information with their national or foreign counterparts.</li> </ul>

## 5.3 Non-Profit Organizations (SR.VIII)

### 5.3.1 Description and Analysis

#### Legal Framework

1065. Any Austrian based, or foreign entity operating in Austria, which claims to be not-for-profit oriented (*gemeinnützig*) can operate under different legal frameworks: association, cooperative society, limited liability company, private foundation or political party. It is estimated that 95 percent of Austrian NPOs are organized in form of an association.

***Review of Adequacy of Laws & Regulations of NPOs (c. VIII.1)***

1066. Various reviews have been conducted by the Austrian authorities, the major study conducted in March and May 2004. This work brought together representatives from the MoF, MoI, MoJ, BVT and the FMA together with the Chamber of Chartered Accountants. The conclusion of the group was that the provisions which were originally established to protect members of NPOs from fraud and wasted donations were appropriate to combat the potential abuse of NPOs for FT purposes.

1067. Group findings are set out in the June 2004 “Review of Non-Profit Organizations Sector in Austria” and concluded that comfort could be taken from the system of disclosures required from the various different types of structures available for NPO formation. The view was that the various disclosures represented reliable sources of information which could be used to identify the size, activities and other relevant features of the NPO sector. This work was re-visited in October 2006 and the initial findings re-affirmed.

1068. Primary sources of information on the activities, size and relevant features of NPOs are public registers and tax records. The authorities point to other sources for data, such as the Seal of Approval Award (*Spendengütesiegel*), the Agency for Austrian Non-for-Profit Associations (*Interessensvertretung Österreichischer Gemeinnütziger Vereine, IÖGV*) -an advocacy and lobbying platform for NPOs in Austria-, and academic research. In addition, pursuant to the DevG, data on cross-border transactions by Austrian NPOs are collected by the Statistics Austria for the OeNB to establish the balance of payments (Article 6, paragraph 4 of the DevG), and classified by type (monetary and other transfers), purpose (education, sports, environment, medical support), and country (origin or destination). Authorities draw also comfort from the fact that the BVT has not reported information gaps while investigating FT cases.

1069. On December 31, 2007, 111,282 associations were registered in Austria. This number includes charitable associations, as well as "activity clubs" (e.g., cooking clubs) and self-help groups. Experts estimate that a large percentage (up to 90 percent) of these associations is small ones. The authorities did not provide information to the assessors regarding the size of financial transactions of the NPO sector, the repartition by type of activities or any information on types of NPOs that are at risk of being misused for FT by virtue of their activities or characteristics. The authorities mentioned that no criminal trials due to terrorist financing in connection with the NPO sector has ever taken place in Austria, and they consider that misuse of NPOs for criminal purposes mostly appears as fraud or the illegitimate use of the means and assets of an association.

***Outreach to the NPO Sector to Protect it from Terrorist Financing Abuse (c. VIII.2)***

1070. Work has been done by the authorities to try to assess the size and risks of the sector and an initial report was produced in mid 2004 following work carried out between March and May of that year involving a great deal of collaboration between various government bodies, charities, donor associations and the Chamber of Chartered Accountants and Tax Consultants. A benchmarking

standard (Seal of Approval Award) has been developed that NPOs may voluntarily seek to gain and be awarded if their governance merits the award. The award is considered to encourage the right kind of provision to reduce the risk of FT, but is a wholly voluntary election on the part of the NPO.

1071. In January 2008, the MoF invited representatives from the NPO sector, auditors, financial institutions, government authorities and private watchdog organizations to a seminar on protecting the NPO sector from being abused for FT purposes. The aim of the seminar was to promote dialogue between the public and private sector, to raise awareness about FT risks and provide examples of preventative measures against possible abuse.

1072. Further opportunities have been sought to promote the importance of adequate defenses and the FMA in particular take the opportunity of meetings with the finance sector to remind them of the importance of vigilance vis-à-vis NPOs. Currently, the FMA are adapting their guidance notes for financial institutions and it is planned to include NPO risks in future versions.

***Supervision or Monitoring of NPOs that Account for Significant Share of the Sector's Resources or International Activities (c. VIII.3)***

***Information maintained by NPOs and availability to the public thereof (c. VIII.3.1)***

1073. Information relating to NPOs' stated activities, or the identity of persons who own, control or direct their activities, including senior officers, board members and trustees is held in accordance with the rules for that type of structure and in the relevant separate registries, or in the case of political parties, with the MoI.

1074. Associations are established through the agreement of statutes, which must contain information inter alia on the name and seat of the association (exclusively in Austria), its purpose, intended activities and means of covering financial needs, membership and other organizational information. The statutes must be submitted to the local district authority or Federal Police Directorate (*Vereinsbehörde*), which may refuse to authorize the foundation of an association if its objectives, name or organization infringe Austrian law. All associations are listed in the ZVR which is administered by the MoI. Information recorded in the ZVR including notably the association's representation as per statutes, the functions and names of the association organ's representatives, is accessible online. Associations must notify the ZVR of any changes regarding their representatives within four weeks (Article 14 VerG). In some cases, a non-disclosure right may be granted because of association interests worth being protected. Every association listed in the ZVR may apply for his data therein being refused to disclose to the public (*Auskunftsperre*) when claiming a case of outstanding endangerment. The application has to be granted if legitimate interest in this measure can be made credible. Such interests may be if an association has references to racial or ethnic origin, political opinion or membership of a trade-union, to religious or philosophical conviction, to health or sexuality.

1075. A private foundation is set up by a declaration of establishment, which documents the legal intent of the founder to dedicate assets for a specific purpose, and must be filed with the Commercial Register. The founding deed, which must be authenticated by a public notary, must indicate the name of the founder/grantor, the scope of the foundation, the names of the members of the board of trustees (who represent the private foundation) and the names of the members of the supervisory board (when

such board is required). The founding deed is maintained by the Commercial Register. The beneficiaries of the foundation can be nominated in the founding deed. However, they may also be designated in an appendix or supplementary declaration to the founding deed, which is not subject to registration at the Commercial Register, nor otherwise accessible to the public.

1076. The Commercial Register contains records about the name and date of birth of the founders, the original shareholders, and managers and directors, as well as the company's statute or the private foundation deed of establishment for all companies and other legal persons. The Register is administered by the Commercial Courts, and information is available on line. Subsequent changes in ownership and control must be registered under penalty of a fine, but only with respect to limited liability companies and joint stock companies with a single shareholder. Each cooperative society must maintain a register of its members, managers and supervisory board members which is open to the public. There is no information on members of cooperative societies in the Commercial Registrar. In addition, the assessors noted that companies with bearer shares do not allow for transparency concerning the beneficial ownership and control of legal persons.

1077. Registration with tax authorities is limited to NPOs active in sectors that are eligible to tax relief on membership fees or qualify donors for tax relief. Those NPOs must be able at all times to justify their eligibility to tax relief, on the basis on information on activities etc. Records must be kept for 7 years. Other NPOs are generally taxable and must also keep records for the assessment of the tax authorities as any other taxable entity and following the same record keeping timeframe.

1078. A political party has to establish statutes which contain information on the organs and representatives of the party. Statutes are published and deposited with the MoI.

***Measures in place to sanction violations of oversight rules by NPOs (c. VIII.3.2)***

1079. There are no specific oversight rules for NPOs, for the reasons set out above. However, the range of sanctions under the various laws controlling company, association or other structures applies. These include being required to close. Given that it is believed the majority of NPOs in Austria are formed as associations, special mention of the sanction powers under the VerG is appropriate. Under Article 31, anyone who:

- a. fails to report the establishment of an association before commencement of activity;
- b. carries on activities without approval;
- c. continues activities after being asked to close;
- d. or when acting as a representative, fails to report changes of statutes, changes of representatives, or address, voluntary liquidation, termination of liquidation, or fails to use the registration number as required;
- e. in the function of a liquidator fails to report the termination of a winding up commits a regulatory offense—unless this offense is brought before the criminal court and will be penalized by the district administration authority or by the local directorate of the federal police respectively, with a fine of up to EUR 218, or in the case of recurrence with a fine of up to EUR 726.

1080. These penalties do not preclude the use of criminal sanction in parallel or as alternatives to these administrative penalties (see also sections of this report addressing Special Recommendation II regarding criminalization of terrorism and Special Recommendation III regarding freezing of assets relating to terrorism). Pursuant to Article 29, paragraph 1 of the VerG, an association can be liquidated if it violates penal laws, infringes the sphere of activity resulting from its statutes, or does not fulfill the conditions of its legal existence.

1081. All other registered NPOs may be fined up to EUR 3,600 by the court if it does not comply with the duty to keep records with the Commercial Register up to date (Article 24 of the FBG). These measures do not preclude any criminal liability (Article 31 of the VerG). Sanctions according to the StGB can be imposed either on the natural persons acting on behalf of the NPO or on the NPO as legal person itself according to the Statute on the Responsibility of Entities for criminal offenses.

***Licensing or registration of NPOs and availability of this information (c. VIII.3.3)***

1082. The legal framework which is in place and relevant to these criteria is mainly the various legal provisions controlling how any organization may be formed and which set out the organizational, filing and reporting obligations. Any Austrian based, or foreign entity operating in Austria, which claims to be not-for-profit oriented (*gemeinnützig*) has to choose a legal status, requiring it to be registered or licensed (in the case of credit cooperatives).

Statistical Table 32. Legal Frameworks for NPOs

Structure type	Public Register	Accounts	Numbers at end 2007
Association	Register of associations ( <i>Vereinsregister</i> )	Y	111,282
Cooperative Societies	Commercial Register ( <i>Firmenbuch</i> )	Y	1,900
Limited Liability Company		Y	110,997
Private Foundation		Y	3,028
Political Party	Lodged with MoI	Y	NA

1083. As indicated above, NPOs which are active in sectors which are eligible to tax relief on membership fees or qualify donors for tax relief have to be registered with the tax authorities.

1084. There is no specific licensing or registration system for NPOs and accordingly there is no central location of information or central location to indicate where the information might be found. The voluntarily sought “Seal of approval Award” cannot be considered a system of licensing or registration as it is entirely elective on the part of the NPO.

***Maintenance of records by NPOs, and availability to appropriate authorities (c. VIII. 3.4)***

1085. There is no standardized set of requirements for the maintenance of NPOs records. NPOs would be required to follow the separate legislative requirements according to the type of structure elected at formation (see description and analysis for R.33 and R.34). According to Article 212 of the Commercial Code (*Unternehmensgesetzbuch, UGB*), every entrepreneur (incl. limited liability

companies and cooperatives) has to keep accounting records for seven years. The same is true for associations and private foundations, as Article 22 VerG and Article 18 PSG refer to Article 212 UGB. Article 132, paragraph 1 of the Federal Fiscal Code (*Bundesabgabenordnung, BAO*) also requires record keeping for 7 years (all NPOs are taxable, even in the case of tax exemption record keeping requirements apply in order to prove that conditions for exemption are met). Article 125 of the Federal Fiscal Code requires that entrepreneurs keep an account of incomes and expenditures from a threshold of a turnover of EUR 400,000 in two consecutive years.

1086. An amendment was introduced in January 2005 to the Associations Act (VerG) requiring that associations with finances exceeding certain thresholds should meet certain additional audit and disclosure obligations. These are based on levels of finance rather than sensitive activities or sensitive jurisdictions. Associations must:

- Prepare financial statements once a year which have to be reviewed by two independent auditors appointed by the association (Article 21 VerG);
- When revenues or expenditures exceed EUR 1 million in each of the previous two years, prepare financial statements have to include a balance sheet and a profit and loss account, which must be certified by two independent auditors (Article 22, paragraph 1 VerG); and
- If revenues or expenditures exceed EUR 3 million in each of the previous two years, prepare financial statements must be certified by a statutory auditor.

1087. Registered companies have to file annual financial statements which are available to the public.

1088. As opposed to corporations, private foundations do not have to file their instruments of accounting (books, balance sheets...) at the company register (*Firmenbuch*) once a year and by this make them known to the public. But it has to disclose information to the tax authorities.

1089. Political parties must keep records of the use of funds and are subject to an annual audit by two accountants. List of donations must be published.

***Measures to ensure effective investigation and gathering of information (c. VIII.4)***

1090. Austria relies also on the investigative powers of its law enforcement authorities, particularly the power to search places, objects and persons set forth by Article 119 of the StPO. This provision allows the search of places (premises that are not publicly accessible) if, due to ascertained facts, it can be assumed that there are objects that have to be seized or examined. The search can be conducted by the criminal police at its own discretion (and then reported as soon as possible to the office of the public prosecutor). The authorities point to the fact that the BVT has already been investigating in FT cases involving NPOs and that no restrictions to access information have been reported.

***Domestic cooperation, coordination and information sharing on NPOs (c. VIII.4.1)***

1091. There are no specific enabling powers to permit domestic cooperation, coordination and information sharing outside the usual criminal investigation framework. Competent authorities can request further information also according to Article 22 of the Federal Constitutional Law

(administrative assistance: “All authorities of the Federation, the *Länder* and the municipalities are bound within the framework of their legal sphere of competence to render each other mutual assistance”).

***Access to information on administration and management of NPOs during investigations (c. VIII.4.2)***

1092. Full access to information on the administration and management of a particular NPO can be obtained during the course of an investigation, as soon as there is a legal basis for the information to be recorded (see c. VIII.3).

***Sharing of information, preventative actions and investigative expertise and capability, with respect NPOs suspected of being exploited for terrorist financing purposes (c. VIII.4.3)***

1093. Opportunities to share information exist at police level (a term which includes the anti terrorist unit) as well as at administrative level, using the mechanisms described in the description and analysis for R.31.

***Responding to international requests regarding NPOs - points of contacts and procedures (c. VIII.5)***

1094. The BVT is the point of contact for information on NPOs that are suspected of terrorist financing or other forms of terrorist support, and information is channeled through it.

**5.3.2 Recommendations and Comments**

1095. Authorities should:

- Require NPOs operating under the legal form of private foundations to make information on the identity of persons who own, control or direct their activities publicly available;
- Strengthen requirements for NPOs to maintain and make available to appropriate authorities records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organization;
- Strengthen outreach to the NPO sector.

**5.3.3 Compliance with Special Recommendation VIII**

	Rating	Summary of factors underlying rating
SR.VIII	PC	<ul style="list-style-type: none"> <li>• NPOs operating under the legal form of private foundations are not required to make information on the identity of persons who own, control or direct their activities publicly available.</li> <li>• NPOs are not adequately required to maintain and make available to appropriate authorities records of domestic and international</li> </ul>

		<p>transactions that are sufficiently detailed.</p> <ul style="list-style-type: none"> <li>• Insufficient outreach exercise.</li> </ul>
--	--	---

## 6. NATIONAL AND INTERNATIONAL COOPERATION

### 6.1 National Cooperation and Coordination (R.31 & R. 32)

#### 6.1.1 Description and Analysis

##### *Mechanisms for Domestic Cooperation and Coordination in AML/CFT (c. 31.1)*

1096. The Federal Constitutional Law states in its Article 22 that “all authorities of the Federation... are bound within the framework of their legal sphere of competence to render each other mutual assistance.” On this basis, various *fora* have been established where competent authorities exchange on AML/CFT issues and coordinate their respective activities.

1097. Pursuant to Article 13 of the FMABG, the Financial Market Committee has competency on financial market’s stability issues, which include AML/CFT matters. This Committee involves senior executive of the MoF, the OeNB and the FMA and is chaired by the MoF representative. It meets at least four times a year, and may adopt recommendations on financial market issues which are considered to have strong policy effects on the ministers and the parliament. In addition, senior representatives of the MoF and the FMA meet on a monthly basis to discuss potential legislative or regulatory actions, as well as operational challenges.

1098. At an operational level, meetings gather a large cross-section of relevant stakeholders who:

- review trends and typologies, operational challenges and private sector issues related to AML/CFT (quarterly AML/CFT Task Force Meetings, with MoF, MoJ, OeNB, FMA, A-FIU, BVT); or
- analyse and discuss AML/CFT policies, supervision and enforcement, in preparation to FATF Plenary meetings (FATF Coordinating Meetings, with MoF, MoJ, MoE, MoFA, OeNB, FMA, A-FIU, BVT).

1099. On financial sector issues, MoF and FMA hold monthly meetings which deal with ongoing issues, operational challenges, or interpretation of legal provisions. For banking activities, the FMA and the OeNB maintain a joint database in which are stored all information collected or received from banks, as well as relevant analysis. Coordination between both institutions has been institutionalized in form of regular meetings at different levels (heads of department, managers) and in the “single bank *fora*”, as well as through the “single points of contact”, FMA and OeNB agents responsible for each supervised entity. Meetings with external auditors are organized on a regular basis to discuss relevant supervisory matters, including AML/CFT.

1100. Article 22 B-VG also enables bilateral cooperation between the A-FIU and other competent authorities. On this basis, the A-FIU receives and forwards relevant information to the competent authorities.

Statistical Table 33. Providers of Information to the A-FIU

	2004	2005	2006	2007
Ministry of Finance	0	27	7	21
FMA	5	2	5	5
Customs	0	0	0	1
<b>Total</b>	<b>5</b>	<b>29</b>	<b>12</b>	<b>27</b>

1101. On the other hand, in the event of STRs containing information relevant to supervisory authorities or if the A-FIU finds reasons to suspect that a reporting entity does not comply with AML/CFT obligations during an investigation or when bank employees are indicted, supervisory authorities are informed. In 2007, the A-FIU forwarded 12 information to the FMA. It has to be noted that the FMA does not request information to the A-FIU on the breakdown of STRs by financial institutions. The A-FIU explained to the assessors that its database would not easily enable to provide such information to the FMA.

1102. Concerning the customs, specific AML/CFT national cooperation is organized pursuant Article 17c (2) ZollR-DG, in connection with the performance of the control of cash brought in to/out of Austria. This article states that the customs authorities must pass the data to the competent authority, these being the ML registration office (A-FIU) for ML and the Federal Office for the Protection of the Constitution and Fight against Terrorism (BVT) for FT, to the extent that this is necessary to perform their statutory tasks.

1103. Concerning FT-related STRs received by the A-FIU, the cooperation between the A-FIU and the BVT is organized according to a BKA circular allowing the immediate transmission of the STR to the BVT. Both the A-FIU and the BVT organize working meetings related to ongoing cases, involving when necessary representatives of other investigative authorities, public prosecutors and court representatives.

***Additional Element - Mechanisms for Consultation between Competent Authorities and Regulated Institutions (c. 31.2)***

1104. In addition to regular contacts and meetings with employees, managers and board members of financial institutions, the FMA has step up its company visit program to increase dialogue on both general and specific issues, focusing notably on AML/CFT questions where relevant.

1105. Consultation took place between DNFBPs representatives and competent ministries in the process of implementing the second and the third EU Directives. Regular meetings are still organized in order to issue AML/CFT guidance (e.g., between the MoJ and the Federal Bar Association). But there is no formal mechanism allowing for regular consultation between the DNFBPs and the competent authorities.

**Statistics (applying R.32)**

1106. No statistics are available up to 2007. In 2008, the FMA issued one request; answer is pending.

**6.1.2 Recommendations and Comments**

1107. The recommendation is fully met.

**6.1.3 Compliance with Recommendations 31 & 32**

	Rating	Summary of factors underlying rating
R.31	C	

**6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)****6.2.1 Description and Analysis*****Ratification of AML Related UN Conventions (c. 35.1)***

1108. Austria signed the Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) on September 25, 1989 and ratified it on July 11, 1997. Austria has declared to interpret Article 3, paragraph 1 and 2 of the Vienna Convention as follows: “in case of a minor nature, the obligations contained in this provision may also be implemented by the creation of administrative penal regulations providing adequate sanction for the offenses enumerated therein.”

1109. Austria signed the United Nations Convention against Transnational Organized Crime (Palermo Convention) on December 12, 2000 and ratified it on September 23, 2004.

**Implementation of Vienna Convention**

1110. Earlier sections of this report show that Austria has enacted legislation that covers the key AML requirements of the Vienna Convention. The elements of the ML offense are largely in line with the physical and material elements of ML as set forth by Article 3(1) (b) and (c) of the Vienna Convention, but the ML offense does not apply to the case of proceeds laundered by the perpetrator of the predicate offense (absence of criminalization of self-laundering). Proper ancillary offenses as well as associated ML are also criminalized by the law.

1111. The trafficking in narcotics and other drug-related offenses are criminalized by Articles 27 (drugs), 28 (large quantities of drugs), 30 (psychotropic substances), 31 (large quantities of psychotropic substances) and 32 (2) (manufacturing a precursor substance) in particular of the Austrian Drug Code (*Suchtmittelgesetz - SMG*).

1112. The criminal laws and the criminal procedure laws provide for provisional measures and for confiscation of proceeds of crime (including proceeds derived from drug related offenses and narcotics and instrumentalities in drug related cases).

1113. Article 99, paragraph 5 StPO makes controlled delivery available under Austrian law. Controlled delivery is governed by the provisions of Section 71 and Section 72 of the Federal law on judicial cooperation in criminal matters with the Member States of the European Union (*Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union, EU-JZG*), which are correspondingly applicable under Article 99, paragraph 5 StPO.

### **Implementation of Palermo Convention**

1114. Earlier sections of this report show that Austria has enacted legislation that covers the key AML requirements of the Palermo Convention (except those dealing with the criminalization of self-laundering). The StGB provides for the offenses of “criminal association” and “criminal organization” (described earlier in this report), as well as appropriate ancillary offenses.

1115. Criminal liability applies also to legal persons. A special form of forfeiture is provided for by Article 20b of the StGB for “property at the disposal of a criminal organization”, however this provision has been applied very rarely.

1116. Law enforcement agencies have a full range of special investigative techniques at their disposal pursuant to the StPO or the SPG; these techniques include observation, undercover investigation, fictitious purchase, monitoring of data, interception of telecommunications, audio-visual monitoring of individuals by technical means and computer-aided data cross-referencing (Articles 134-143 StPO).

1117. For the issues related to confiscation and identifications and tracing of proceeds of crime, see chapter 2.

### ***Ratification of CFT Related UN Conventions (c. I.1)***

1118. Austria signed the 1999 International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention, TFC) on September 24, 2001 and ratified it on April 15, 2002.

### **Implementation of Terrorist Financing Convention**

1119. Earlier sections of this report show that Austria has enacted legislation that has encompassed the key AML requirements of the TFC. The provisions of Article 2(1)(a) of the TFC have been implemented by Article 278d(1)-(7) StGB in a way which is largely in line with Article 2 of the TFC. However, because of the issues discussed earlier in the report (exclusion of criminality envisaged by Article 278c, paragraph 3<sup>44</sup> of the StGB; cases in which FT is only a misdemeanor) organization and direction of others is not fully in line with the 1999 UN convention; nor is it the contribution to the

---

<sup>44</sup> Article 278c, paragraph 3 introduces an exclusion of criminality for the offenses considered as terrorist acts listed in paragraph 1, because it states that “the offence is not regarded as terrorist criminal offence if it is directed to the establishment or re-establishment of a democratic and constitutional situation or the exercise or observance of human rights.” In this case, the offenses are not considered “terrorist criminal offences” under Article 278c and are punished according to the penalties set forth by the specific provisions of the StGB. This exclusion of criminality was criticized by the UN Sanction Committee.

commission of FT by a group of persons in the case in which the sole purpose/activity of the group of persons is FT. Therefore the offense of FT as defined by Article 278d of the StGB adequately covers the material elements of FT set forth under Article 2, paragraph 1(a) and (b) and paragraph 5(a) of the TFC, but it does not cover in all instances the direction and organization of others and the contribution to of a group of persons acting with a common purpose (as required by Article 2, paragraphs 5(b) and (c), when organization/direction is solely for FT and when the group of persons has only FT as a common purpose. Legal persons may also be held criminally liable of FT.

1120. The FT offense applies if the provision or collection of assets takes place in Austria, irrespective of the place where the terrorist act is, or planned to be, committed. If the FT offense itself was committed abroad, according to Section 64, paragraph 1(10), Austria can take jurisdiction only if either: (i) the perpetrator has been an Austrian at the time of the offense or he/she has gained the Austrian citizenship afterwards and is still in its possession at the time of the institution of criminal proceedings; or (ii) the perpetrator has been a foreigner at the time of the offense, but at the time of prosecution is in Austria and cannot be extradited.

1121. Austria is party to all the treaties listed in the annex of the TFC and has implemented in its domestic criminal law the offenses set thereof; however the exclusion of criminality envisaged by Article 278c, paragraph 3 for terrorist acts is not in line with Article 6 of the TFC.

***Implementation of UN SCRs relating to Prevention and Suppression of FT (c. I.2)***

1122. Mechanisms have been put in place for the implementation of UNSCRs 1267 and 1373 (for details see analysis under SR.III); however the freezing obligations regarding assets other than funds are not fully covered; the OeNB regulations adopted pursuant to the Exchange of Control Act (for EU-internal terrorists) do not constitute freezing mechanisms in the terms required by UNSCR 1373 and SR.III.

***Additional Element—Ratification or Implementation of Other relevant international conventions (c. 35.2)***

1123. Austria signed the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime on July 10, 1991 and ratified it on July 7, 1997.

1124. Austria is not a party of the Inter-American Convention.

**6.2.2 Recommendations and Comments**

1125. The authorities are recommended to:

- Criminalize self laundering;
- Soften the requirements for law enforcement authorities to obtain access to information subject to secrecy;
- Extend the criminalization to the whole range of activities envisaged by Article 2, paragraphs 5(b) and (c) of the 1999 UN Convention;

- Set up procedures within Austria that will ensure freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles); and
- Modify the OeNB regulations adopted pursuant to the Exchange of Control Act (for EU-internal terrorists) in order to make possible freezing of funds and assets held by EU-internals in all instances set forth by UNSCR 1373 and SR.III.

### 6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	LC	<ul style="list-style-type: none"> <li>• Self-laundering is not criminalized in Austria.</li> <li>• Strict conditions for obtaining/compelling information subject to secrecy which hinder the possibility for law enforcement authorities to locate and trace property.</li> <li>• Criminal provisions not fully in line with the 1999 UN Convention.</li> </ul>
SR.I	PC	<ul style="list-style-type: none"> <li>• Criminalization of organization and direction of others is not fully in line with the 1999 UN convention, nor is it the contribution to the commission of FT by a group of persons in those instances where the sole purpose/activity of the group of persons is FT.</li> <li>• Incomplete implementation of UNSCRs 1267 and 1373.</li> </ul>

## 6.3 Mutual Legal Assistance (R.36-38, SR.V)

### 6.3.1 Description and Analysis

#### Legal Framework

1126. The type and extent of international cooperation that Austria may provide is mainly regulated by the Federal Law on Extradition and Mutual Assistance in Criminal Matters (*Auslieferungs- und Rechtshilfegesetz, ARHG*), the international conventions to which Austria is party, and by other multilateral and bilateral agreements concluded.

#### *Widest Possible Range of Mutual Assistance (c. 36.1)*

1127. Pursuant to Articles 1 and 3, paragraphs 1 and 50 of the ARHG, Austria may provide a range of measures of mutual assistance in AML (and CFT) investigations, prosecutions and related proceedings initiated by other countries. Judicial assistance may indeed be granted in criminal matters upon a request by a foreign authority, including proceedings to order preventive measures and to issue a property-law order, as well as in matters of extinction and the register of criminal records, in proceedings to obtain compensation for confinement and conviction by a criminal court, in clemency petition matters and in matters concerning the execution of sentences and measures. More specifically, the measures that may be taken upon request of another country include:

- the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons (under the conditions described under criterion 36.5 below);
- the taking of evidence or statements from persons;
- providing originals or copies of relevant documents and records as well as any other information and evidentiary items;
- effecting service of judicial documents;
- facilitating the voluntary appearance of persons for the purpose of providing information or testimony to the requesting country; and
- identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for FT, as well as the instrumentalities of such offenses, and assets of corresponding value.

1128. These measures may be granted on the basis of multilateral or bilateral agreements as well as, where no such agreement exists, on the basis of reciprocity. In cases there are any doubts concerning reciprocity, the opinion of the MoJ must be sought (Article 3, paragraph 3 of the ARHG).

1129. The Department for International Criminal Cases within the MoJ performs the function of the central authorities for sending and receiving MLA and extradition requests. Immediately upon reception of request, the Department forwards the case to the competent executing authority. All incoming requests are also registered in a countrywide computer system to which all prosecutors and all courts have access. The system allows for the identification, tracing and monitoring of all mutual legal assistance requests.

1130. In many cases, the incoming requests are addressed directly to the competent prosecutor's office or to the competent court on the basis of the Convention implementing the Schengen Agreement, the Convention between the Member States of the EU on Mutual Assistance in Criminal Matters, the Framework Decision on the execution in the EU of orders freezing property or evidence or the EU Framework Decision on the application of the principle of mutual recognition to confiscation orders, or on the basis of a bilateral treaty providing for direct contacts between the competent authorities.

***Provision of Assistance in Timely, Constructive and Effective Manner (c. 36.1.1)***

1131. According to the authorities, the requests are forwarded to the competent authority without delay and processed in a timely fashion. This is in line with the general requirement set out in the StPO (to which Article 9, paragraph 1 of the ARHG refers), more precisely its Article 9, paragraph 1 which ensures that criminal proceedings are being conducted “within a reasonable timeframe” (“*innerhalb angemessener Frist*”) and that the proceedings are always conducted “rapidly and without undue delay” (“*stets zügig und ohne unnötige Verzögerung*”).

1132. Information obtained from other FATF members indicates that in most cases, the mutual legal assistance requests are dealt with within a 2 weeks to a few months timeframe. While most members indicated general satisfaction with the MLA granted, others found the process somewhat

slow. The authorities did not provide further information establishing that assistance is provided in **all cases** in a timely manner.

***No Unreasonable or Unduly Restrictive Conditions on Mutual Assistance (c. 36.2)***

1133. Pursuant to Article 51 of the ARHG, the provision of judicial assistance is not admissible to the extent that:

- the act underlying the request is either not subject to punishment by a court under Austrian law or does not qualify for extradition;
- extradition would be inadmissible because:
  1. the criminal proceedings, punishment or preventive measures in the requesting State will not comply or did not comply with the principles of Articles 3 (prohibition of torture, inhuman or degrading treatment or punishment) and 6 (right to a fair trial) of the Convention for the Protection of Human Rights and Fundamental Freedoms (Human Rights Convention); or
  2. the person to be extradited would be subject to persecution in the requesting State because of his/her origin, race, religion, affiliation to a specific ethnic or social group, nationality, or political opinions, or would have to expect other serious prejudices for any of these reasons (extradition asylum).;
- the practical requirements to perform specific investigative measures, as defined in Title 8 of the StPO, do not prevail, or providing judicial assistance would result in a violation of the obligation to confidentiality, to be also observed vis-à-vis criminal courts under Austrian law (Article 76, paragraph 2 of the StPO).

***Efficiency of Processes (c. 36.3)***

1134. As mentioned above, the main gateway for incoming requests is the Department of International Criminal Cases of the MoJ. The Department is competent for forwarding the cases to the relevant authorities.

1135. Quicker procedures have also been established by enabling to requesting authority to address its request directly to its Austrian counterpart. Under several bilateral MLA-treaties concluded by Austria, the requesting authority may address its request directly to its Austrian counterpart. This is also valid for requests for extradition (“surrender”), as well as for requests for MLA in the relations between the Member States of the EU (see e.g., Framework Decision on the European Arrest Warrant as well as the instruments mentioned under point 1083 which have all been implemented by the Federal Law on Judicial Cooperation in Criminal Matters with the Member States of the EU, EU-JZG).

1136. Austria has concluded bilateral treaties with all its neighboring States, in addition to signing the European Convention on Mutual Assistance in Criminal Matters of April 20, 1959. These treaties establish a direct channel of communication between the requesting and the executing judicial authorities of both States. Furthermore the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 (established by the Council in accordance with Article 34 of the Treaty on European Union) also allows for direct communication.

In urgent cases the channel granted by the national INTERPOL/SIRENE Bureaux can be used to transmit request for assistance.

1137. In all cases, the proceedings must be conducted expeditiously and without undue delay (“*stets zügig und ohne unnötige Verzögerung*”) pursuant to Article 9, paragraph 1 ARHG which refers to the StPO, and, *in casu*, its Article 9, paragraph 1.

1138. The Public Prosecutor’s Office is responsible for the execution of foreign requests. The work related to and the execution of these requests are supervised by the Public Prosecutor’s Office at the Court of Appeals. Public Prosecutors Offices must report to the MoJ of all instances where the assistance has been denied.

1139. Any complaint against the length of the execution or the efficiency of the outcome of the requested assistance is handled by the MoJ. The relevant Prosecutor’s Office must then inform the MoJ of any delay or shortcoming including steps and motions undertaken to execute the request. The MoJ is empowered to give orders to Public Prosecutors Offices.

***Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 36.4)***

1140. The provision of mutual legal assistance is not admissible when the punishable acts underlying the request are exclusively of a fiscal nature (Article 51, paragraph 1, no. 1 and 15 no. 2 of the ARHG). Austria may however grant mutual legal assistance for other types of offenses, regardless of whether they are also considered to involve fiscal matters (Article 15 no. 2 of the ARHG).

***Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 36.5)***

1141. Access to banking information ordinarily covered by confidentiality requirements is enabled by the Austrian criminal procedure law: Article 116 of the StPO provides that the disclosure of information on bank accounts and bank operations is admitted on the basis of a court order “if it seems to be necessary to clarify a criminal offense or misdemeanor under the jurisdiction of the Regional courts” (which includes offenses such as ML of FT). Although primarily aimed at domestic criminal proceedings, this provision also serves the purposes of MLA (Article 9, paragraph 1 of the ARHG). The foreign request for information is to be addressed to the public prosecutor’s office, which then seeks a court order for disclosure of all relevant material. The court need only satisfy itself that there is a link between the information sought and the offenses investigated or prosecuted, and that the information will be used solely for the purpose of these proceedings or investigations.

1142. Article 38 of the BWG mentions that the secrecy requirement does not apply when a court requests information’s from banks for the purpose of an ongoing criminal proceedings. Article 38 of the BWG provides the legal basis for lifting the banking secrecy, while Article 116 of the StPO specifies the procedural requirements for obtaining information on bank accounts and bank operations. The conditions set out in Article 116 of the StPO are however fairly restrictive in the sense that the prosecution must establish on the basis of “particular circumstances” that the information sought is linked to a criminal offense (see write-up under Recommendation 4 for further information). This renders the lifting of the banking secrecy cumbersome and slows down the provision of MLA.

1143. Access to information held by insurance undertakings and securities firms is granted to the A-FIU on the basis of Article 98f, paragraph 2 of the VAG and Articles 6 and 12, paragraph 4 of the WAG. All requests for information will, therefore, have to be forwarded to the A-FIU for execution.

***Availability of Powers of Competent Authorities (applying R.28, c. 36.6)***

1144. All the powers granted to the relevant authorities in domestic cases and described in the write-up for Recommendation 27 may be made available for use in response to requests for mutual legal assistance (Article 9, paragraph 1 of the ARHG stipulates that the provisions of the StPO are applicable to mutual legal assistance proceedings unless specified otherwise).

***Avoiding Conflicts of Jurisdiction (c. 36.7)***

1145. No general mechanism has been devised to deal with conflict of jurisdictions. Pursuant to the rule of legality and the accusatory principle (“*Legalitätsprinzip*, and *Offizialprinzip*”), the Austrian prosecutor must investigate and prosecute any crime that falls within the jurisdiction of the Austrian courts. Conflicts of jurisdiction are dealt with on a case-by-case basis, although the authorities maintain that this is not a frequent occurrence.

***Additional Element—Availability of Powers of Competent Authorities Required under R28 (c. 36.8)***

1146. The investigative powers at the Austrian authorities’ disposal under Recommendation 28 are also available when there is a direct request from a foreign judicial or law enforcement authority (Article 9, paragraph 1 of the ARHG). However the shortcomings noted in regard to access to information protection by secrecy, discussed under Recommendation 28 (and Recommendation 3) may affect the provision to foreign authorities of information that is covered by secrecy.

***International Cooperation under SR V (applying c. 36.1-36.6 in R. 36, c. V.1) & Additional Element under SR V (applying c. 36.7 & 36.8 in R.36, c. V.6)***

1147. The provisions described above apply equally to the fight against terrorism and terrorist financing.

***Dual Criminality and Mutual Assistance (c. 37.1, 37.2 & V.2)***

1148. Dual criminality applies as a general rule when mutual legal assistance is granted on the basis of the ARHG, that is, in the absence of an applicable multilateral or bilateral treaty (Article 51, paragraph 1 sub-paragraph 1 ARHG). Exceptions to the dual criminality requirement are set forth in Article 49a of the Convention implementing the Schengen Agreement, in the Convention between the Member States of the EU on Mutual Assistance in Criminal Matters, the Framework Decision on the execution in the EU of orders freezing property or evidence and the EU Framework Decision on the application of the principle of mutual recognition to confiscation orders as well as in several bilateral MLA-Treaties.

1149. The absence of dual criminality is not an obstacle to the service of documents if the recipient is prepared to accept them (Article 51, paragraph 2 of the ARHG). This does not however apply to

documents covered by the banking secrecy (which can only be lifted under the conditions mentioned in the write-up for Recommendations 4 and 36 above).

***Timeliness to Requests for Provisional Measures including Confiscation (c. 38.1 & V.3)***

1150. Chapter III of the ARHG provides the legal basis for the execution of foreign criminal court decisions, including foreign confiscation orders and provisional measures. Article 64, paragraph 1 sets out the general prerequisites in these terms:

“(1) The execution or further execution of a decision by a foreign court imposing a fine or custodial sentence, a preventive measure or property-law order with final and enforceable effect shall be admissible upon a request by another State if:

1. the decision of the foreign court was taken in proceedings complying with the principles set forth in Article 6 of the [Human Rights Convention],
2. the decision was taken for an act that is sanctioned by a court punishment under Austrian law,
3. the decision was not taken for one of the punishable acts listed in § 14 and § 15 [i.e., military offenses and offenses that are exclusively of fiscal nature],
4. under Austrian law no statute of limitation applies to the execution,
5. the person concerned by the decision of the foreign court is not prosecuted for an act in Austria, has not been convicted or acquitted with final an enforceable effect or otherwise been exempted from prosecution.”

1151. This enables the Austrian authorities, on request of a foreign State, to identify, seize, freeze and confiscate all relevant assets. *Vermögensrechtliche Anordnungen*, or “property-law orders”, deals not only with immovable, but also other types of assets, including the laundered property and proceeds of a ML of FT offenses, as well as the instrumentalities used in or intended to be used in the commission of these offenses and of the predicate crimes.

1152. The procedure is simplified among EU members: Article 45 to 51 of the EU-JZG provide for the execution of seizing and freezing orders following the rules of the FD of July 22, 2003, OJ L 196 of August 2, 2003, p. 45. Article 52 EU-JZG provides for the execution of confiscation orders by Member States in accordance with the rules set out in the FD of October 6, 2006 on the application of the principle of mutual recognition to confiscation orders, OJ L 328 of November 24, 2006, p. 59. These instruments allow a speedy procedure using a certificate to forward the request. The principle of dual criminality is not assessed if the crime appears in the list of crimes as set out in the FD mentioned above.

***Property of Corresponding Value (c. 38.2 & V.3)***

1153. Requests relating to property of corresponding value are dealt with in a similar way as described above, on the basis of the ARHG and, when the requesting State is another member of the EU, the EU-JZG.

***Coordination of Seizure and Confiscation Actions (c. 38.3)***

1154. There is no general agreement for the coordination of seizure and confiscation actions. The authorities indicated however that such an agreement is not a pre-condition for coordination and that, in practice, the law enforcement authorities have coordinated their actions in a number of cases.

***International Cooperation under SR V (applying c. 38.1-38.3 in R. 38, c. V.3)***

1155. The MLA provisions described above apply in the same way when the request deals with terrorist financing.

***Asset Forfeiture Fund (c. 38.4)***

1156. Pursuant to Article 64, paragraph 7 of the ARHG forfeited or confiscated assets fall into the Federal budget. No special fund was established.

***Sharing of Confiscated Assets (c. 38.5)***

1157. Asset sharing between EU Member States is made possible under Article 53, paragraph 1 of the EU-JZG whenever the confiscated assets are higher than EUR 10,000. Furthermore, Austria is in the process of concluding an asset sharing agreement with the United States. As far as other countries are concerned (i.e., countries other than the other EU Member States and the United States), a separate bilateral treaty would have to be concluded to enable the sharing of confiscated assets.

***Additional Element (R 38) – Recognition of Foreign Orders for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture; and, c) Confiscation of Property which Reverses Burden of Proof (applying c. 3.7 in R.3, c. 38.6)***

1158. The Austrian legal framework does not provide the possibility to enforce foreign non-criminal confiscation orders, nor to reverse the burden of proof.

***Additional Element under SR V (applying c. 38.4-38.6 in R. 38, c V.7)***

1159. The answers provided above for ML proceedings are equally valid in the fight against FT.

***Statistics (applying R.32)***

1160. There are no comprehensive statistics available on the type of measures and the timeframe between the receipt of the request and its execution. Every incoming foreign request is registered in the nationwide electronic file register system (“VJ”). This system can be accessed by every Austrian judicial authority. According to the authorities, it allows an effective monitoring of every foreign mutual legal assistance request.

**6.3.2 Recommendations and Comments**

1161. The authorities should:

**Recommendation 36**

- Ensure that MLA is granted in a timely manner and ensure that requirements to lift banking secrecy and the scope of legal privilege do not slow down effective cooperation.

**Recommendation 38**

- Conclude arrangements for coordinating seizure and confiscation actions with other countries.
- Consider sharing of confiscated assets with countries other than EU members and the United States.
- Ensure that MLA is granted in a timely, constructive and effective manner.
- Remove from banking secrecy provisions all requirements which may hinder effective cooperation.

**Recommendation 37**

- Remove from banking secrecy provisions all requirements which may hinder effective cooperation.

**SR.V**

- Ensure that requirements to lift banking secrecy and the scope of legal privilege do not slow down effective cooperation.

**6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V**

	<b>Rating</b>	<b>Summary of factors relevant to s.6.3 underlying overall rating</b>
<b>R.36</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Practice indicates that MLA may not always be granted in a timely manner.</li> <li>• Deficiencies noted under Recommendation 1 (absence of criminalization of self-laundering and incomplete list of predicates) narrow the scope of the MLA that Austria may grant.</li> <li>• Strict requirements to lift banking secrecy and extensive scope of legal privilege slow down effective cooperation.</li> </ul>
<b>R.37</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Effectiveness not established.</li> </ul>
<b>R.38</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Strict requirements to lift banking secrecy and extensive scope of legal privilege slow down effective cooperation.</li> <li>• Deficiencies noted under Recommendation 1 (absence of criminalization of self-laundering and incomplete list of predicates) narrow the scope of the</li> </ul>

		<p>MLA that Austria may grant.</p> <ul style="list-style-type: none"> <li>• No arrangements in place for coordinating seizure and confiscation actions with other countries.</li> <li>• No consideration given to sharing of confiscated assets with countries other than EU members and the United States.</li> <li>• Effectiveness not established.</li> </ul>
<b>SR.V</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Strict requirements to lift banking secrecy and extensive scope of legal privilege slow down effective cooperation.</li> <li>• Effectiveness not established.</li> </ul>

#### **6.4 Extradition (R.37, 39, SR.V)**

##### **6.4.1 Description and Analysis**

###### **Legal Framework**

1162. The general provisions on extradition may be found the ARHG “insofar as intergovernmental agreement do not stipulate otherwise” (Article 1 of the ARHG). Intergovernmental agreements that provide otherwise include European decisions which facilitate the extradition procedure among EU Members.

###### ***Dual Criminality and Mutual Assistance (c. 37.1 & 37.2)***

1163. Mutual legal assistance usually cannot be rendered in the absence of dual criminality. However, where bilateral agreements have been signed, such as those concluded between Austrian and Switzerland, or multilateral agreements have been concluded, such as the Convention Implementing the Schengen Agreement (CISA) and the Convention on Mutual Assistance in Criminal Matters between Member States of the EU, the assistance may be rendered even in the absence of dual criminality.

###### ***Money Laundering and Terrorist Financing as Extraditable Offenses (c. 39.1 & SR V.4)***

1164. ML as set out in Article 165 StGB is an extraditable offense under Austrian law. As mentioned under Recommendations 1 and 2 however, the offense only covers third-party laundering. Extradition may therefore not be granted when the offense which is being prosecuted abroad is self-laundering.

1165. Terrorist financing is also an extraditable offense.

1166. The extradition procedure is similar to that for other types of crimes and is regulated by the ARHG and the relevant bilateral and multilateral treaties in extradition such as: the EU Convention on Extradition and its second Additional Protocol of 1978; the EU Framework Decision on the

European arrest warrant and the surrender procedures between EU Member States of 2002, which Austria implemented in its Federal Law on Judicial cooperation in criminal matters with members States of the EU (*Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union; EU-JZG*); as well as other applicable international conventions dealing with extradition to which Austria is party.

1167. Pursuant to Article 30 of the ARHG, extradition request are to be addressed to the MoJ. The latter conducts an initial study of the request and, in the absence grounds for refusal, forwards the request to the competent public prosecutor's office for processing. Constitute grounds for refusal by the MoJ requests that violate the public order or other essential interest of Austria, or instances where reciprocity is not ensured.

1168. Article 11 of the ARHG sets out the general rule for the provision of extradition which applies to all types of criminal proceedings, including those dealing with ML or FT. It provides that extradition may be granted:

- for the prosecution of intentionally committed acts that are punishable under the law of the requesting State by a custodial sentence of more than one year or by a preventive measure of the same duration and that are subject to a custodial sentence of more than one year under Austrian law.
- in cases where the custodial sentence or the preventive measure has been imposed for one or several of the punishable acts listed above and when a remaining period of at least four months still needs to be executed.

1169. The ARGH further provides for a number of exemptions to this general rule by stating that extradition may not be granted:

- when the person whose extradition is sought is an Austrian national (Article 12, paragraph 1 of the ARHG);
- for political offenses (Article 14, paragraph 1 of the ARHG);
- for other punishable acts that are based on political motives or aims, unless the criminal nature of the act outweighs its political natures (Article 14, paragraph 2 of the ARHG);
- for acts that are exclusively of a military nature (Article 15, no. 1 of the ARHG);
- for punishable acts that are subject to Austrian jurisdiction (Article 16, paragraph 1 of the ARHG, with the exceptions noted under paragraphs 2 and 3);
- when the person has been acquitted by a court of the State in which the offense was committed or has otherwise been exempted from prosecution (Article 17 no. 1 of the ARHG);
- when the person has been convicted by a court in a third country, and the punishment has been fully served or waived in whole or in part for the portion of the sentence remaining to be enforced, or if the enforceability of the punishment comes under the statute of limitation pursuant to the law of this third country (Article 17 no. 2 of the ARHG);
- if prosecution or execution come under the statute of limitation;

- the criminal proceedings in the requesting State will not comply or did not comply with the principles of [...] 6 (right to a fair trial) of the Human Rights Convention;
- the punishment or preventive measure imposed by or to be expected in the requesting State would be enforced in a manner that is not consistent with the requirements of Article 3 (prohibition of torture, inhuman or degrading treatment or punishment) of the Human Rights Convention;
- the person to be extradited would be subject to persecution in the requesting State because of his/her origin, race, religion, affiliation to a specific ethnic or social group, nationality, or political opinions, or would have to expect other serious prejudices for any of these reasons (extradition asylum);
- for execution of the death penalty or other punishments or preventive measures that do not comply with the requirements of Article 3 of the Human rights convention mentioned above (Article 20 of the ARHG);
- when the person whose extradition is sought was without criminal responsibility at the time of the punishable act (Article 21 of the ARHG);
- when the person whose extradition is sought would be exposed to hardship, that is, to obviously disproportionately severe conditions when considering the severity of the punishable act with which he or she is charged, his or her young age, the long period of his or her residence in Austria, or other serious reasons based on his or her personal circumstances (Article 22 of the ARHG).

1170. While the grounds for refusal indicated above seem reasonable, the law includes an additional ground, which unduly narrows the scope of MLA as far as the fight against ML is concerned: Article 15 no. 2 of the ARHG indicates that a request for extradition is inadmissible “for acts that constitute a violation of stipulations relating to taxes, monopolies or customs duties, or foreign exchange regulations, or of stipulations relating to the control of or foreign trade in goods.” This entails that, although smuggling is a predicate offense to ML under Austrian law, extradition cannot be granted when the underlying offense is a violation of customs duties.

1171. Anecdotal evidence indicates that Austria refused to cooperate with Turkey by extraditing Riza Altun, a Turkish national, member of the PKK and subject of an Interpol arrest warrant, and enabled Riza Altun to evade judicial measures. Turkey filed a complaint against Austria to the UN Counter Terrorism Committee by letter to its chairman dated July 24, 2007, as well as to other international for a such as the OSCE. Austria’s grounds for refusal were not shared with the assessors.

***Statistics (applying R.32)***

1172. In 2006, Austria surrendered 183 persons under a European Arrest Warrant to other EU Member States. 20 European Arrest Warrants were refused by Austrian judicial authorities. The surrender procedure takes in average 23 days, where the person agreed to the surrender, and 47 days, where the person did not consent to the surrender. The extradition procedure in relation to other countries takes in average 63 days, where the person was held in custody. 47 persons have been surrendered to other countries. No further details were provided.

***Extradition of Nationals (c. 39.2 & SR V. 4) & Cooperation for Prosecution of Nationals (applying c. 39.2(b), c. 39.3 & SR V. 4)***

1173. Extradition of Austrian nationals is not admissible pursuant to Article 12, paragraph 1 of the ARHG. The authorities mentioned that this provision has the rank of a constitutional provision and, as such, requires a 2/3 majority of Parliament to be amended. Nevertheless, as of January 1, 2009, Austria will be in a position to extradite its own nationals to other EU-Member States in accordance with Section 5 EU-JZG.

1174. Where extradition for ML is denied on the sole ground of nationality, the Austrian courts are competent under Article 65, paragraph 1, no. 1 of the StGB (jurisdiction over acts committed by Austrians abroad) and must conduct the proceedings in the same way as for any other criminal offense under national law. The Austrian courts also have explicit jurisdiction over terrorist acts and terrorist financing when the perpetrator is Austrian (Article 64, paragraph 1, nos. 9 and 10 of the StGB).

1175. Cooperation between the Austrian and the foreign authorities is ensured on the basis of bilateral or multilateral agreements to which Austria is party, in particular the Council of Europe Convention on MLA of 1957 and its Additional Protocol of 1978, the EU Convention on Mutual Assistance in Criminal Matters between Member States of the EU of 2000, as well as on the basis of other international conventions that contain provisions on MLA. In the absence of such agreements, Austria may cooperate with other countries on the basis of reciprocity under the ARHG.

***Efficiency of Extradition Process (c. 39.4 & SR V.4)***

1176. In the absence of any contrary provision in the ARHG, the provisions of the StPO apply pursuant to Article 9, paragraph 1 ARHG, and in particular Article 9, paragraph 1 StPO, which ensures the defendant the right to criminal proceedings to be conducted within a reasonable timeframe (“*innerhalb angemessener Frist*”) and the proceedings are always to be conducted rapidly and without undue delay (“*stets zügig und ohne unnötige Verzögerung*”).

1177. No information was provided on the practical implementation of these requirements in extradition cases.

***Additional Element (R.39 & SR V)—Existence of Simplified Procedures relating to Extradition (c. 39.5 & SR v.8)***

1178. A simplified procedure is possible under Article 32 of the ARHG when a person consents to the extradition and to being transferred without the need for the requesting State to conduct a formal extradition proceeding. In the absence of any contradictory provisions, the simplified procedure may also apply when the crime for which a person is being extradited is ML or FT.

1179. Further, a simplified procedure was also established among member States of the EU in the form of the European arrest warrant (pursuant to the EU Framework Decision on the European arrest warrant and the surrender procedures between Member States of 2002, which was implemented by Austria through Article 30, paragraph 1 of the EU-JZG).

**Statistics (applying R.32)**

1180. According to the authorities, statistics on the number of extraditions requested and granted exist, but they are not broken down per type of underlying offense and were not provided to the assessors.

**6.4.2 Recommendations and Comments**

1181. The authorities should:

- Take steps to improve the overall effectiveness of the extradition framework.

**6.4.3 Compliance with Recommendations 37 & 39, and Special Recommendation V**

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
<b>R.39</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Lack of evidence of the overall effectiveness of the extradition framework.</li> </ul>
<b>R.37</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Effectiveness not established.</li> </ul>
<b>SR.V</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Effectiveness of the extradition framework not established.</li> </ul>

**6.5 Other Forms of International Cooperation (R.40 & SR.V)****6.5.1 Description and Analysis****Legal Framework****A-FIU and Other Law Enforcement Authorities**

1182. The legal framework for cooperation of the Austrian police, including the A-FIU and the BVT, is mainly described in the Police Cooperation Act (*PolizeiKooperationsgesetz, PolKG*). Pursuant to Article 3(1) of the PolKG, the law enforcement authorities are obliged to render legal assistance upon request of a foreign law enforcement authority on condition of reciprocity. In addition, the EU Council Decision of October 17, 2000 (2000/642/JHA) concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information establishes standards for the cooperation between FIUs in EU Member States. The Interpol Statutes and the Europol Convention are also applicable.

**Supervisory Authorities**

1183. In the context of administrative assistance, the provision of information or documents is allowed to the extent that this is necessary for the consolidated supervision of cross-border financial holding companies and mixed-activity holding companies (Directive 2006/48/EC) or financial institutions in financial conglomerates (Directive 2002/87/EC). The consolidated supervision covers operational risk which include ML and FT risks. The FMA can provide information and documents to competent authorities (Article 77, paragraph 5 of the BWG):

- in EEA Member States;
- in third countries with which the EU has concluded a agreement regarding the means of exercising consolidated supervision; and
- in other third countries with which cooperation is in the interest of the Austrian supervisor and in compliance with international standards.

1184. Information may be provided under the following conditions:

- the provision of information is necessary for conducting supervision of a consolidated basis;
- professional secrecy rules are applied; and
- passing on information is subject to express consent by the authorities which communicated it initially.

1185. Apart from administrative assistance, communication of official information by the FMA to foreign banking supervisory authorities is permitted (Article 77, paragraph 1 of the BWG):

- if the public order, other essential interests of the Republic of Austria, banking secrecy or confidentiality obligations under tax law are not violated;
- if it is ensured that the requesting government would fulfill an Austrian request of the same kind; and
- if a request for information of a similar nature by the FMA would be in line with the objectives of the BWG.

1186. Pursuant to Article 97, paragraph 1 of the WAG, the FMA should act as the Austrian contact point for the purpose of EU Directive 2004/39/EC for the securities business. According to Article 56, paragraph 1 of the Directive, competent authorities in Member States must render assistance to each other and “exchange information and cooperate in any investigation or supervisory activities.” In addition, Article 91, paragraph 5 and 6 of the WAG provides that data can be transmitted to competent authorities in EU Member states and in third countries, on condition that these authorities perform tasks “equivalent to the FMA’s tasks”, and that data are subject to professional secrecy rules.

1187. For the insurance sector, “perceptions based on the supervision of the business activities”, whether information or documents, may be made available to supervisory authorities in third countries (Article 118, paragraph 1 of the VAG), providing that reciprocity is granted, and that information and documents will be used for supervisory purposes only and communicated to third parties under conditions equivalent to Austrian law.

### ***Widest Range of International Cooperation (c. 40.1)***

#### ***Provision of Assistance in Timely, Constructive and Effective Manner (c. 40.1.1)***

#### **A-FIU And Other Law Enforcement Authorities**

1188. Pursuant to Article 3 of the PolKG (which is also applicable to the Police and the BVT), the A-FIU can provide information to any foreign Security police authority. The legal department of the Ministry of Interior confirmed that, irrespective of their administrative or law enforcement type,

financial intelligence units have to be considered as Security police authorities. Consequently, the A-FIU is allowed to exchange information with any foreign FIU based on reciprocity. The term “foreign security police authority” is defined in Article 2, paragraph 3 PolKG<sup>45</sup>.

1189. The request of the foreign counterpart has to be translated in German, which may add some delays in the exchange of information. According to the authorities, the average time required for translation is about 15 days, but flexible solutions can be found in case of urgent requests.

### **Supervisory Authorities**

1190. The legal framework defines a cooperation regime that allows the FMA to exchange information generally for the supervision of groups of financial institutions, including domestic financial institutions. The AVG, which regulates the supervision of domestic financial institutions, has no provision regarding international cooperation.

### ***Clear and Effective Gateways for Exchange of Information (c. 40.2):***

#### **A-FIU**

1191. The A-FIU is a member of the Egmont group and uses frequently the Egmont secure web (ESW) to exchange information. Unless a case has already been opened, the A-FIU has to be authorized by the foreign counterpart to open a criminal investigation in Austria in order to answer a request not limited to the search of its databases.

### **Supervisory Authorities**

1192. The FMA has signed a large number of MoUs with foreign supervisors which strengthen operative cross-border cooperation, notably with CESE countries where Austrian financial institutions are particularly active: 14 bilateral agreements have been concluded for the credit and domestic financial institutions, 6 for the insurance activities and 6 for the securities business. The coverage of CESE and CIS is still limited and in the near future, the focus will be on entering into MoUs with some relevant non-EU countries. Austria is also part to EU supervisory arrangements (CEIOPS, CESR, ECB, CEBS etc).

1193. Bilateral meetings are regularly held with foreign supervisors (9 meetings in 2007) to address issues of cross border supervision. In addition, the FMA participated in or organized cooperation meetings or supervisory colleges where home and host supervisors of a financial institution meet to exchange information and coordinate supervisory actions (6 meetings in 2007). While mostly geared towards enhancing prudential supervision, they prove to be useful channel for AML/CFT cooperation as well.

### ***Spontaneous Exchange of Information (c. 40.3)***

---

<sup>45</sup> Article 2 paragraph 3 PolKG reads “Foreign security authorities are other states’ agencies which exercise tasks in compliance with Article 1 paragraph 1 PolKG, including authorities responsible for threat assessment as part of safeguarding the internal security of the state.” Article 1 paragraph 1 reads: “International cooperation serves the purpose of 1. Security police, 2. Criminal Investigation Division, 3. Passport authorities, aliens police, and border control..”

### **A-FIU and Other Law Enforcement Agencies**

1194. Pursuant to Article 3(2) PolKG, the A-FIU and the BVT are empowered to exchange information without being requested with other law enforcement organizations. In the case of FIUs of the EU Member States, the A-FIU can spontaneously exchange information regarding to financial transactions related to ML and the natural or legal persons involved, pursuant to Article 1(2) of the EU Council Decision 2000/642/JHA. The authorities mentioned that information exchange is not possible in the case of self-laundering, as it is not criminalized in Austria.

### **Supervisory Authorities**

1195. The supervisory authorities provide information spontaneously during institutionalized meetings, notably at the EU level or in the context of MoUs, as well through direct contacts with their foreign counterparts.

### ***Making Inquiries on Behalf of Foreign Counterparts (c. 40.4)***

#### **Supervisory Authorities**

1196. When a foreign authority requests the FMA to verify information related to a credit or a domestic financial institution registered in Austria, the FMA may, pursuant to Article 77, paragraph 6 of the BWG:

- authorize the foreign authority to conduct, or to participate in, the verification;
- delegate the verification to the OeNB; or
- instruct external auditors to carry out the verification.

1197. Home supervisors may inspect domestic branches of foreign insurance undertakings, as soon as the FMA has been notified in writing (Article 102a, paragraph 3 of the VAG). The FMA may participate in those inspections or appoint other inspecting bodies.

1198. When the FMA receives a request from a securities supervisor in other EU Member State, it may carry out the verification or investigation or allow the foreign authority or auditors to carry out the verification or investigation (Article 98, paragraph 1 of the WAG). It may refuse a request when it may adversely affect the sovereignty, security or public order of Austria, judicial processing have been initiated or a judgment has been delivered in Austria on the same basis, against the same person (Article 99, paragraph 1 of the WAG). There are no provisions authorizing Austrian authorities to conduct inquiries on behalf on securities supervisors from third countries, beyond Article 91, paragraph 6 of the WAG which permits the transmission of data.

### ***FIU Authorized to Make Inquiries on Behalf of Foreign Counterparts (c. 40.4.1)***

1199. Pursuant to Article 5 of the PolKG, the A-FIU is authorized to search its own databases on behalf of foreign counterparts. This includes information related to STRs and the search of other databases to which it has direct or indirect access. In case an investigation is not already opened in Austria, the A-FIU has to be authorized by the foreign FIU to open an investigation in order to answer a request not limited to the search of its databases. This is consistent with the StPO that requires an investigation to be open when there is a suspicion of a criminal offense.

***Conducting of Investigations on Behalf of Foreign Counterparts (c. 40.5)***

1200. The same provision applies to the BVT and the Police

***No Unreasonable or Unduly Restrictive Conditions on Exchange of Information (c. 40.6)*****A-FIU**

1201. The A-FIU is only authorized to conduct investigations initiated by inquiries from abroad if the requesting authority permits the A-FIU to make use of the information sent in its own criminal investigation.

**Supervisory Authorities**

1202. **Credit institutions:** the provision of information and documents is allowed in the context of administrative assistance to competent authorities in EU Member States, and in third countries either which have entered into a consolidated supervision agreement with the EU Council, or with which cooperation is necessary in the interest of Austrian banking supervision, in line with international standards (Article 77, paragraph 5 of the BWG). The information exchange must serve the purpose of fulfilling the duties of the competent authorities, and is subject to the conditions of professional secrecy defined in Article 44 of the Directive 2006/48/EC.

1203. In case the above provisions do not apply, Article 77, paragraph 1 of the BWG allow the FMA to provide foreign supervisory authorities with official information subject to the following conditions:

- the public order, other essential interests of the Republic of Austria, banking secrecy or confidentiality obligations under tax law (Article 48 Federal Tax Code) are not violated;
- reciprocity is ensured, and
- the request is in line with the objectives of the BWG.

1204. **Insurance undertakings:** the FMA is entitled to provide information and documents to foreign supervisory authorities about domestic subsidiaries of foreign undertakings (Article 118, paragraph 1 and Article 118a of the VAG). The VAG lists information and documents that can be provided (Article 118, paragraph 2, and Article 118a, paragraph 1), and includes information and documents about shareholders, and members of the management and supervisory boards, or related to the supervisory of the business. Information and documents are for supervisory purposes only and subject to confidentiality rules equivalent Austrian's rules.

1205. **Securities institutions:** The WAG gives the FMA power to provide information to supervisory authorities in other EU Member States if information is (i) required to discharge their duties; and (ii) subject to professional secrecy (Article 97, paragraph 2). Similar conditions apply to the transmission of data to authorities in third countries (Article 91, paragraph 6 of the BWG).

***Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 40.7)*****A-FIU**

1206. The A-FIU only refuses cooperation in cases in which the request concerns exclusively fiscal matters. Cooperation can be granted when the request involves fiscal matters among others.

**Supervisory Authorities**

1207. The authorities declare that requests for cooperation to the FMA cannot be refused on the sole ground that they also involve fiscal matters.

***Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 40.8)*****A-FIU**

1208. As soon as an investigation has been opened for ML, the A-FIU is empowered to access information from financial institutions and DNFBPs and can exchange this information with foreign counterparts. Concerning lawyers, notaries and accountants, the extent of the notion of ‘legal advice’ may prevent the provision of international cooperation (see discussion in section 4).

**Supervisory Authorities**

1209. **Credit institutions:** the provision of information to competent authorities in EU Member States, and in third countries under a consolidated supervision agreement or in the interest of Austrian banking supervision is subject professional secrecy as defined in Article 44 of Directive 2006/48/EC. The provision of official information to other countries is allowed, notably, if banking secrecy is not violated (Article 77, paragraph 1 of the BWG). Inquiries are assessed on a case-by-case basis. Until now, no request has been denied.

1210. **Insurance undertakings:** information and documents given to foreign authorities are subject to confidentiality rules equivalent Austrian’s rules.

1211. **Securities institutions:** provision of information to EU Member States’ supervisory authorities is subject to professional secrecy (Article 97, paragraph 1 of the WAG). The legal provisions do not address other counterparts with which the FMA may cooperate and exchange information.

***Safeguards in Use of Exchanged Information (c. 40.9)*****A-FIU**

1212. As soon as the information request from a foreign FIU relates to a suspicion of ML or an underlying predicate offense, an investigation has to be opened, pursuant to the Criminal procedure code. Consequently, the exchanged information will be treated as protected by the same provisions as apply to similar information obtained from domestic sources. When the preliminary proceedings ends or the case is final, the suspect/defendant can be authorized to view all the files related to the investigation, including the request from a foreign FIU, as discussed under the analysis for c.13.1.

**Supervisory Authorities** (see above)**Effectiveness**

1213. The authorities reported that there were few cases where foreign authorities requested information related to AML/CFT supervision, and no request has been denied. No statistics are available.

***Additional Element—Exchange of Information with Non-Counterparts (c. 40.10 & c. 40.10.1)*****A-FIU**

1214. The EU Council Decision 2000/642/JHA gives a legal basis for the A-FIU to exchange information with FIUs from EU Member States that are not law enforcement agencies, and are consequently not considered as counterparts according to the PolKG.

**Supervisory Authorities**

1215. There are no provisions allowing the direct exchange of information with non-counterparts. Requests for information from non-counterparts would be processed indirectly through other foreign or domestic authorities.

***Additional Element—Provision of Information to FIU by Other Competent Authorities pursuant to request from Foreign FIU (c. 40.11)***

1216. Pursuant to the PolKG and the EU Council Decision 2000/642/JHA, the A-FIU can obtain information requested by EU and law enforcement FIUs from other competent authorities or other persons, including from reporting entities. In practice, the A-FIU informed the assessors that any FIU in the world would receive the requested information from the A-FIU provided it gives the permission to make use of the data initially provided.

***International Cooperation under SR V (applying c. 40.1-40.9 in R. 40, c. V.5)*****A-FIU/BVT**

1217. The BVT is the sole responsible agency concerning FT. The BVT is not a member of the Egmont Group and there is no specific mention regarding FT-related international cooperation in the letter sent by the BKA to the BVT in June 2003 regarding the procedure to combat FT. But the authorities informed the assessors that FT-related international cooperation is done by the A-FIU on behalf of the BVT. The BVT is a member of several working groups at the international level, among others the Police Working Group on Terrorism (PWGT), an informal group of police services dedicated to the fight against terrorism. The aim of this group, to which the BVT also belongs, is to exchange situation reports and experience, to rapidly convey information on special cases and to directly coordinate and align operational measures.

1218. Anecdotal evidence indicates that Austria refused to cooperate with Turkey by extraditing Riza Altun, a Turkish national, member of the PKK and subject of an Interpol arrest warrant, and enabled Riza Altun to evade judicial measures. Turkey filed a complaint against Austria to the UN

Counter Terrorism Committee by letter to its chairman dated July 24, 2007, as well as to other international for a such as the OSCE. Austria's grounds for refusal were not shared with the assessors.

### Supervisory Authorities

1219. Rules and procedures for information exchange, which apply in the context of prudential supervision of operational risk, include FT risk.

#### *Additional Element under SR V (applying c. 40.10-40.11 in R. 40, c. V.9)*

1220. The A-FIU is not competent for FT-related international cooperation. See reference to BVT under relevant criteria.

#### *Statistics (applying R.32)*

### FIU

1221. The following table summarizes information on the use of the Egmont Secure Web (ESW) by the A-FIU:

Statistical Table 34. Information Received or Sent Through the ESW

	2005	2006	2007
Information requested by foreign FIUs	166	159	195
Requests sent by the A-FIU	43	65	188
<b>Total</b>	<b>209</b>	<b>224</b>	<b>383</b>

Statistical Table 35. Breakdown of Information Requested by Foreign FIUs

Country	2006	2007
Belgium	5	
Belize		2
Bolivia	4	
Bulgaria	14	
Croatia	17	2
Cyprus		2
Denmark	4	
Germany	6	10
Hungary	12	
Italy		4
Liechtenstein	7	
Lithuania		2
Luxembourg		2
Russian Federation	8	3
Serbia-Montenegro	4	
Slovakia	17	

Slovenia		3
Switzerland	11	5
UK		5
Ukraine		2
USA		2
Others	46	21
<b>Total</b>	<b>109</b>	<b>44</b>

## MLA

1222. The MoJ maintains statistics on the number of incoming requests for MLA, but they are not sufficiently comprehensive to establish the type of measures requested and the timeframe within which the Austrian authorities respond to the request.

### Supervisory Authorities

1223. No statistics are available up to 2007. In 2008, the FMA issued one request; answer is pending.

#### *Rec 30 for MLA:*

1224. The MoJ Department for International Criminal Cases is the central authority for the receiving incoming request for MLA and extradition. It is composed of one head of Department and four lawyers which are all either judges or prosecutors. The department is equipped with a computer system which enables the tracing of all MLA and extradition proceedings and the status of domestic proceedings pending before the court of the prosecution services. The department also has access to the electronic register of residents and the register of persons in custody.

1225. Staff of the Department takes part in trainings and seminars on the fight against ML and FT. The courses are offered either by the EU institutions (such as EUROPOL, EUROJUST, OLAF), the Academy of European law in Trier (Germany) or by the domestic authorities.

### 6.5.2 Recommendations and Comments

1226. The authorities should:

#### FIU

- Grant the A-FIU the sufficient resources in order to respond to foreign FIU requests in a timely way;
- Enable the A-FIU to exchange information on FT.

#### Supervisory authorities

- Establish provisions which allow competent authorities to conduct inquiries on behalf of securities supervisors from third countries.

### 6.5.3 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relative to s.6.5 underlying overall rating
--	--------	--

<b>R.40</b>	<b>LC</b>	<u>FIU</u> <ul style="list-style-type: none"> <li>• A-FIU lacking resources may delay the response to some requests depending on the circumstances.</li> </ul> <u>Supervisory authorities</u> <ul style="list-style-type: none"> <li>• Lack of provisions as regards to conducting inquiries on behalf of securities supervisors from third countries.</li> </ul>
<b>SR.V</b>	<b>NC</b>	<u>FIU</u> <ul style="list-style-type: none"> <li>• A-FIU not legally empowered to exchange information on FT</li> </ul>

## 7. OTHER ISSUES

### 7.1 Resources and Statistics

1227. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report that is, sections 2, 3, 4, and 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report contains the boxes showing the rating and the factors underlying the rating.

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R.30</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Additional resources required in the police and supervisory areas, especially in the DNFBP sector (besides legal professions).</li> <li>• Need for strengthened AML/CFT training for supervisors, especially in the DNFBP sector (besides legal professions).</li> </ul>
<b>R.32</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• No statistics available on the number of extraditions.</li> <li>• Insufficient statistics on information exchange between supervisory authorities.</li> <li>• No data about domestic financial institutions' supervision.</li> <li>• Lack of data on MLA.</li> </ul>

**Table 1. Ratings of Compliance with FATF Recommendations**

Forty Recommendations	Rating	Summary of factors underlying rating <sup>46</sup>
<b>Legal systems</b>		
1. ML offense	<b>LC</b>	<ul style="list-style-type: none"> <li>• No confirmation that the non-criminalization of self-laundering is supported by principles that amount to fundamental principles according to the FATF standard.</li> <li>• Low number of convictions and indictments for ML compared to the number of ML criminal investigations and convictions for serious offenses that generate proceeds in Austria, and standard of proof required by the courts to establish that assets originate from crime indicating an issue of effectiveness in the implementation of the ML criminal provision.</li> <li>• Counterfeiting and piracy of products not predicate offenses for ML.</li> </ul>
2. ML offense—mental element and corporate liability	<b>LC</b>	<ul style="list-style-type: none"> <li>• Sanctions for ML against natural persons and minimum sanction established in the case of legal persons too lenient and not effective, proportionate or dissuasive.</li> <li>• Low number of convictions and indictments for ML compared to the number of ML criminal investigations and convictions for serious offenses that generate proceeds.</li> </ul>
3. Confiscation and provisional measures	<b>PC</b>	<ul style="list-style-type: none"> <li>• Strict conditions for obtaining/compelling information subject to banking secrecy and scope of legal privilege hinder the possibility for law enforcement authorities to locate and trace property.</li> <li>• Given the level of profit-generating crimes, effective use of the provisional measures and confiscation provisions not demonstrated.</li> </ul>
<b>Preventive measures</b>		

<sup>46</sup> These factors are only required to be set out when the rating is less than Compliant.

4. Secrecy laws consistent with the Recommendations	<b>PC</b>	<ul style="list-style-type: none"> <li>• Disclosure of banking information under Article 116, paragraph 3, lit. b StPO is subject to restrictive conditions which hamper access to relevant information in practice.</li> </ul>
5. Customer due diligence	<b>PC</b>	<ul style="list-style-type: none"> <li>• Undue exemption from CDD measures for customers that are credit institutions established in EU member countries.</li> <li>• Undue blanket exemption from CDD measures for fiduciary accounts that amount to less than EUR 15,000.</li> <li>• No requirement to apply beneficial owner's identification and verification diligence to holders of savings documents for savings deposit accounts which balance is lower than EUR 15,000 and are not registered in the customer's name.</li> <li>• Current list of suggested high-risk customers omits some significant high risk business categories relevant to Austria.</li> <li>• No guidelines issued by the competent authorities on the extent of the CDD measures on a risk sensitive basis.</li> <li>• Effectiveness was not established for some criteria.</li> </ul>
6. Politically exposed persons	<b>LC</b>	<ul style="list-style-type: none"> <li>• Measures in place limited to customers who fit the definition of a PEP at the beginning of a business relationship only.</li> <li>• Effectiveness was not established.</li> </ul>
7. Correspondent banking	<b>LC</b>	<ul style="list-style-type: none"> <li>• Undue exemption from additional measures for correspondent relationships with credit institutions established in EEA member countries.</li> </ul>
8. New technologies and non-face-to-face business	<b>LC</b>	<ul style="list-style-type: none"> <li>• No requirement for financial institutions to have policies in place or to take measures to prevent the misuse of technological developments in ML/FT schemes.</li> </ul>
9. Third parties and introducers	<b>LC</b>	<ul style="list-style-type: none"> <li>• Presumption that all EU and EEA countries adequately apply the FATF recommendations.</li> </ul>
10. Record-keeping	<b>C</b>	

11. Unusual transactions	<b>PC</b>	<ul style="list-style-type: none"> <li>• No explicit requirement in laws, regulations or other enforceable means to examine as far as possible the background and purpose of all complex, unusual large transactions, or patterns of transactions, that have no apparent or visible economic or lawful purpose, to set forth findings in writing and to keep such findings for at least five years.</li> <li>• Monitoring of unusual patterns of transactions not required for insurance undertakings.</li> <li>• Concerns about the effectiveness of the provisions which were introduced recently.</li> </ul>
12. DNFBP–R.5, 6, 8–11	<b>PC</b>	<p><u>All DNFBPs:</u></p> <ul style="list-style-type: none"> <li>• Some shortcomings in the requirements concerning PEPs.</li> </ul> <p><u>Casinos:</u></p> <ul style="list-style-type: none"> <li>• Absence of AML/CFT requirements for all casinos operating in Austria.</li> <li>• No legal framework for CDD requirements concerning internet casinos.</li> <li>• No rules to determine the basis upon which internet casinos are subject to AML/CFT requirements.</li> <li>• No legal obligation for casinos to perform CDD for all customers when they engage in financial transactions equal to or above EUR 3,000.</li> <li>• No specific review for higher risk categories and no enhanced due diligence for higher risk categories of customers, such as non-resident customers.</li> <li>• No legal obligation of record keeping of transactions.</li> <li>• No enforceable requirements for Internet casinos in order to address the specific risks related to non-face-to-face transactions.</li> <li>• No appropriate management systems to determine whether a potential customer, a customer or the beneficial owner is a PEP.</li> </ul>

	<p><u>Real estate agents, dealers and TCSPs:</u></p> <ul style="list-style-type: none"> <li>• Coverage of TCSP activities is not effective.</li> <li>• No requirement to verify that any person purporting to act on behalf of the customer is so authorized.</li> <li>• No guidelines issued to determine the extent of the CDD measures on a risk sensitive basis.</li> <li>• No specific review for higher risk categories and no enhanced due diligence for higher risk categories of customers, such as non-resident customers.</li> <li>• Weaknesses of the simplified CDD framework.</li> <li>• No requirement to keep written findings of the examination of complex and unusual transactions.</li> <li>• Lack of effective implementation of the CDD requirements.</li> </ul> <p><u>Lawyers and notaries:</u></p> <ul style="list-style-type: none"> <li>• The scope of the CDD requirements is unclear.</li> <li>• The identification and verification of the beneficial owner is not systematic.</li> <li>• Absence of enhanced due diligence required for higher risk categories.</li> <li>• Weaknesses of the simplified CDD framework.</li> <li>• Absence of requirements concerning existing customers.</li> <li>• No requirement to pay special attention to all complex and unusual transactions.</li> <li>• Extent of the CDD requirements is limited by the wide definition of the legal privilege.</li> <li>• Effective implementation limited by the absence of guidance for lawyers.</li> </ul> <p><u>Accountants:</u></p> <ul style="list-style-type: none"> <li>• Scope of the CDD requirements unclear for accountants regulated by the WT-ARL.</li> <li>• Limitation of the general CDD requirements</li> </ul>
--	---

		<p>due to a reference to risk.</p> <ul style="list-style-type: none"> <li>• The identification and verification of the beneficial owner is not systematic.</li> <li>• Extent of the CDD requirements is limited by the wide definition of the legal privilege.</li> <li>• Weaknesses of the simplified CDD framework.</li> <li>• No requirement to keep written findings of the examination of complex and unusual transactions.</li> <li>• Lack of effective implementation of the CDD requirements.</li> </ul>
13. Suspicious transaction reporting	<b>PC</b>	<ul style="list-style-type: none"> <li>• Reporting requirement not on funds that are the proceeds of a criminal activity, but limited to transactions that serve the purpose of ML.</li> <li>• No requirement to make an STR regarding funds that are the proceeds of piracy or counterfeiting. The GewO does not require to report STRs in case of self-laundering.</li> <li>• Provisions in three of the four different reporting laws raise technical issues that could affect institutions' decisions on whether they are obliged to file reports in relation to FT in certain situations.</li> <li>• Effectiveness questions raised by the low level of STRs.</li> </ul>
14. Protection and no tipping-off	<b>LC</b>	<ul style="list-style-type: none"> <li>• The protection for STR reporting applies in the absence of good faith for insurance intermediaries.</li> <li>• The possibility to refer the customer to the police when a transaction is suspended creates an indirect "tipping off."</li> </ul>
15. Internal controls, compliance and audit	<b>PC</b>	<ul style="list-style-type: none"> <li>• No ad-hoc provision in law, regulation or other enforceable means giving the compliance officer right to access CDD data and information, transaction records and other relevant information;</li> <li>• Lack of specific provisions establishing that the compliance officer is a management position.</li> </ul>

		<ul style="list-style-type: none"> <li>• No requirement for domestic financial institutions to maintain an internal audit function.</li> <li>• Insufficient integration of AML/CFT compliance into internal audit work for securities and insurance business.</li> <li>• Inadequate staff screening requirements and practices.</li> </ul>
16. DNFBP–R.13–15 and 21	<b>PC</b>	<p><u>All DNFBPs</u></p> <ul style="list-style-type: none"> <li>• Scope of STRs too narrow.</li> <li>• Effectiveness questions raised by the extremely low level of STRs.</li> <li>• No requirements to give special attention to business relationships and transactions with persons from countries insufficiently applying the FATF recommendations.</li> </ul> <p><u>Casinos</u></p> <ul style="list-style-type: none"> <li>• No requirements for internet casinos.</li> </ul> <p><u>Real estate agents, dealers and TCSPs</u></p> <ul style="list-style-type: none"> <li>• Absence of effective coverage of TCSPs.</li> </ul> <p><u>Lawyers and notaries</u></p> <ul style="list-style-type: none"> <li>• Scope of the legal privilege severely limiting the requirement to report STRs.</li> </ul> <p><u>Accountants</u></p> <ul style="list-style-type: none"> <li>• Scope of the legal privilege severely limiting the requirement to report STRs.</li> </ul>
17. Sanctions	<b>PC</b>	<ul style="list-style-type: none"> <li>• Sanctions not sufficiently proportionate and dissuasive.</li> <li>• No sanctions for senior management besides sanctions for criminal liability.</li> <li>• Limited effectiveness.</li> </ul>
18. Shell banks	<b>C</b>	
19. Other forms of reporting	<b>C</b>	
20. Other NFBP and secure transaction techniques	<b>LC</b>	<ul style="list-style-type: none"> <li>• Insufficient measures to reduce the relative importance of use of cash and large denomination banknotes.</li> </ul>

21. Special attention for higher risk countries	<b>PC</b>	<ul style="list-style-type: none"> <li>• No specific requirement in law, regulation or other enforceable means to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations.</li> <li>• No explicit requirement in laws, regulations or other enforceable means to examine as far as possible the background and purpose of transactions with persons from those countries, which have no apparent economic or visible lawful purpose, to set forth and keep findings.</li> </ul>
22. Foreign branches and subsidiaries	<b>LC</b>	<ul style="list-style-type: none"> <li>• Obligation to apply equivalent AML/CFT provisions limited to CDD and record keeping measures.</li> </ul>
23. Regulation, supervision and monitoring	<b>PC</b>	<ul style="list-style-type: none"> <li>• Assessment of significant or controlling interest in a financial institution undermined by capital hold in form of bearer shares.</li> <li>• Insufficient licensing requirements or other legal or regulatory measures which would prevent criminals to control domestic financial institutions, and lack of adequate fit and proper test for their directors and senior managers.</li> <li>• No requirements to carry out fit and proper tests of senior managers and supervisory board members in all types of financial institutions.</li> <li>• Low number of onsite examinations for AML/CFT compliance.</li> <li>• Effectiveness of AML/CFT supervision of domestic financial institutions was not established.</li> </ul>
24. DNFBP—regulation, supervision and monitoring	<b>PC</b>	<ul style="list-style-type: none"> <li>• Absence of adequate powers to perform supervision of internet casinos.</li> <li>• Absence of power to control the beneficial owners of a significant or controlling interest in casinos, and to prevent actions by associates of criminals.</li> <li>• Absence of systems for monitoring and ensuring compliance with AML/CFT requirements for accountants and all the companies active in the TCSP sector.</li> </ul>

		<ul style="list-style-type: none"> <li>• Lack of effectiveness and resources to implement the measures envisaged by the GewO.</li> <li>• Inadequate sanctioning powers.</li> </ul>
25. Guidelines and Feedback	<b>LC</b>	<ul style="list-style-type: none"> <li>• No up-to- date guidance on reporting for credit and domestic financial institutions, insurance undertakings, and securities institutions.</li> <li>• Insufficient guidance available to industry on the new legal requirements.</li> <li>• Absence of guidelines for all DNFBPs but notaries and casinos.</li> <li>• Limited general feedback tailored to the specific needs of each DNFBPs, and absence of systematic case by case feedback on STRs.</li> </ul>
<b>Institutional and other measures</b>		
26. The FIU	<b>PC</b>	<ul style="list-style-type: none"> <li>• A-FIU not a national centre for analyzing and disseminating STRs.</li> <li>• A-FIU not a national centre for receiving, analyzing and disseminating information concerning suspected FT activities other than STRs.</li> </ul>
27. Law enforcement authorities	<b>C</b>	
28. Powers of competent authorities	<b>LC</b>	<ul style="list-style-type: none"> <li>• Strict conditions for obtaining/compelling information subject to banking secrecy and scope of legal privilege hinder the possibility for law enforcement authorities to locate and trace property.</li> </ul>
29. Supervisors	<b>LC</b>	<ul style="list-style-type: none"> <li>• Low level of AML/CFT supervision of domestic financial institutions.</li> <li>• No supervisory powers of sanction against a domestic financial institution.</li> </ul>
30. Resources, integrity, and training	<b>LC</b>	<ul style="list-style-type: none"> <li>• Additional resources required in the police and supervisory areas, notably for the DNFBP sector.</li> <li>• Need for strengthened AML/CFT training for supervisors, especially in the DNFBP sector.</li> </ul>

31. National cooperation	<b>C</b>	
32. Statistics	<b>PC</b>	<ul style="list-style-type: none"> <li>• No statistics available on the number of extraditions.</li> <li>• Insufficient statistics on information exchange between supervisory authorities.</li> <li>• No data about domestic financial institutions' supervision.</li> <li>• Lack of data on MLA.</li> </ul>
33. Legal persons–beneficial owners	<b>PC</b>	<ul style="list-style-type: none"> <li>• Insufficient capacity to ascertain beneficial ownership in the case of companies that issue bearer shares and, in some instances, in the case of private foundations.</li> <li>• Competent authorities not always able to obtain or access to adequate, accurate and current information on the beneficial ownership and control of legal persons in a timely fashion.</li> <li>• No risk assessment undertaken by the authorities to ascertain the risk of ML/FT in the case of joint stock companies which have issued bearer shares, nor in the case of foundations, where the founding deed does not indicate the name of the beneficiaries.</li> </ul>
34. Legal arrangements – beneficial owners	<b>PC</b>	<ul style="list-style-type: none"> <li>• No transparency where the property held in <i>Treuhand</i> is composed of assets other than funds (regardless of the <i>Treuhänder</i>); where the <i>Treuhänder</i> is someone other than a lawyer, notary or registered TSP; where funds held under <i>Treuhand</i> by lawyers amount to less than the federal state threshold (i.e., between EUR 15,000 and EUR 40,000).</li> <li>• No transparency over foreign trusts operated from Austria.</li> <li>• No effective AML/CFT oversight to ensure TSPs properly obtain, verify and record details of the <i>Treuhand</i> and its beneficial ownership.</li> <li>• No effective means by which bodies charged with the oversight of TSPs for AML/CFT purposes can share information with their national or foreign counterparts.</li> </ul>
<b>International Cooperation</b>		

35. Conventions	<b>LC</b>	<ul style="list-style-type: none"> <li>• Self-laundering is not criminalized in Austria.</li> <li>• Strict conditions for obtaining/compelling information subject to secrecy and extensive scope of legal privilege hinder the possibility for law enforcement authorities to locate and trace property.</li> <li>• Criminal provisions not fully in line with the 1999 UN Convention.</li> </ul>
36. Mutual legal assistance (MLA)	<b>PC</b>	<ul style="list-style-type: none"> <li>• Practice indicates that MLA may not always be granted in a timely manner.</li> <li>• Deficiencies noted under Recommendation 1 (absence of criminalization of self-laundering and incomplete list of predicates) narrow the scope of the MLA that Austria may grant.</li> <li>• Strict requirements to lift banking secrecy and extensive scope of legal privilege slow down effective cooperation.</li> </ul>
37. Dual criminality	<b>LC</b>	<ul style="list-style-type: none"> <li>• Effectiveness not established.</li> </ul>
38. MLA on confiscation and freezing	<b>PC</b>	<ul style="list-style-type: none"> <li>• Strict requirements to lift banking secrecy and extensive of legal privilege slow down effective cooperation.</li> <li>• Deficiencies noted under Recommendation 1 (absence of criminalization of self-laundering and incomplete list of predicates) narrow the scope of the MLA that Austria may grant.</li> <li>• No arrangements concluded for seizure and confiscation actions with other countries.</li> <li>• No consideration given to sharing of confiscated assets with countries other than EU members and the United States.</li> <li>• Effectiveness not established.</li> </ul>
39. Extradition	<b>LC</b>	<ul style="list-style-type: none"> <li>• Lack of evidence of the overall effectiveness of the extradition framework.</li> </ul>
40. Other forms of cooperation	<b>LC</b>	<p data-bbox="846 1717 898 1749"><u>FIU</u></p> <ul style="list-style-type: none"> <li>• A-FIU lacking resources may delay the response to some requests depending on the circumstances.</li> </ul>

		<p><u>Supervisory authorities</u></p> <ul style="list-style-type: none"> <li>• Lack of provisions as regards to conducting inquiries on behalf of securities supervisors from third countries.</li> </ul>
<b>Nine Special Recommendations</b>		
SR. I Implement UN instruments	<b>PC</b>	<ul style="list-style-type: none"> <li>• Criminalization of organization and direction of others is not fully in line with the 1999 UN convention, nor is it the contribution to the commission of FT by a group of persons in those instances where the sole purpose/activity of the group of persons is FT.</li> <li>• Incomplete implementation of UNSCRs 1267 and 1373.</li> </ul>
SR.II Criminalize terrorist financing	<b>PC</b>	<ul style="list-style-type: none"> <li>• The offense of FT not fully applicable in all the circumstances envisaged by SR.II, because in the case of the financing of a terrorist organization or an individual terrorist, the provision and collection of funds <i>per se</i> may not constitute an offense if it cannot be established that the provision or collection was with the knowledge that the assets were intended to be used for the commission of terrorist acts and in some other circumstances.</li> <li>• Penalties too low and possible need for a link to a specific offense for penalty purposes.</li> <li>• Criminalization of organization and direction of others not fully in line with the 1999 UN Convention.</li> </ul>
SR.III Freeze and confiscate terrorist assets	<b>PC</b>	<ul style="list-style-type: none"> <li>• Lack of effective procedures to allow freezing or to freeze without delay in the case of assets other than funds in many instances.</li> <li>• The OeNB regulations adopted pursuant to the DevG (for EU-internal terrorists) do not constitute freezing mechanisms in the terms required by UNSCR 1373 and SR.III, because they are mainly applicable to non residents and they do not encompass the full range of the economic resources.</li> <li>• Insufficient guidance provided to financial institutions and other persons or entities concerning their obligations under freezing</li> </ul>

		mechanisms.
SR.IV Suspicious transaction reporting	<b>LC</b>	<ul style="list-style-type: none"> <li>• Provisions in three of the four different reporting laws raise technical issues that could affect institutions' decisions on whether they are obliged to file reports in certain situations.</li> </ul>
SR.V International cooperation	<b>PC</b>	<ul style="list-style-type: none"> <li>• Strict requirements to lift banking secrecy and extensive scope of legal privilege slow down effective cooperation.</li> <li>• A-FIU not legally empowered to exchange information on FT.</li> <li>• Effectiveness not established.</li> </ul>
SR.VI AML/CFT requirements for money/value transfer services	<b>LC</b>	<ul style="list-style-type: none"> <li>• Deficiencies in the framework for preventive measures.</li> </ul>
SR.VII Wire transfer rules	<b>C</b>	
SR.VIII Nonprofit organizations	<b>PC</b>	<ul style="list-style-type: none"> <li>• NPOs operating under the legal form of private foundations are not required to make information on the identity of persons who own, control or direct their activities publicly available.</li> <li>• NPOs are not adequately required to maintain and make available to appropriate authorities records of domestic and international transactions that are sufficiently detailed.</li> <li>• Insufficient outreach exercise.</li> </ul>
SR.IX Cross Border Declaration and Disclosure	<b>PC</b>	<ul style="list-style-type: none"> <li>• Exception from the declaration/disclosure obligations for the municipalities of Jungholz and Mittelberg not in line with the requirements of SR.IX.</li> <li>• Lack of monitoring and checks of cross border transportation of cash into Jungholz and Mittelberg posing a serious risk of ML.</li> <li>• Implementation of the declaration/disclosure requirements not effective.</li> </ul>

**Table 2. Recommended Action Plan to Improve the AML/CFT System**

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
<b>1. General</b>	
<b>2. Legal System and Related Institutional Measures</b>	
2.1 Criminalization of Money Laundering (R.1, 2, and 32)	<ul style="list-style-type: none"> <li>• Criminalize self-laundering.</li> <li>• Make counterfeiting and piracy of products predicate offense to ML.</li> <li>• Undertake actions (awareness raising or training) that would alter the kind of proof currently deemed necessary to show that property is proceeds or that conduct resulted in proceeds so that it will not be necessary for a successful prosecution that the prosecutor provides evidence that a specific offence occurred or a specific perpetrator engaged in the conduct.</li> <li>• Increase the penalties set forth for natural persons by Article 165 and the minimum sanctions applicable in the case of legal persons.</li> </ul>
2.2 Criminalization of Terrorist Financing (SR.II and R.32)	<ul style="list-style-type: none"> <li>• Extend the criminalization of FT in all instances envisaged in SR.II with reference to the financing of terrorist organizations and the individual terrorist, regardless of whether that financing is for criminal activities, legal activities or general support.</li> <li>• Extend the criminalization to the whole range of activities envisaged by Article 2, paragraphs 5(b) and (c) of the 1999 UN Convention.</li> <li>• Increase the penalties set forth for FT.</li> </ul>
2.3 Confiscation, freezing, and seizing of proceeds of crime (R.3 and 32)	<ul style="list-style-type: none"> <li>• Ease the requirements for law enforcement authorities to obtain access to information held by financial institutions and lawyers and notaries.</li> <li>• Consider the changes that need to be made in order to ease the burden in establishing that an organization is a “criminal organization” or otherwise change provisions so that Article 20b, when applied in the case of property at the disposal of such organizations, is more readily enforceable.</li> <li>• Improve the effectiveness of the provisions by using them more frequently to restrain and confiscate criminal assets for ML, FT and predicate crimes, especially by making more use of forfeiture.</li> <li>• Maintain more precise statistics on amounts restrained and</li> </ul>

	confiscated in each instance.
2.4 Freezing of funds used for terrorist financing (SR.III and R.32)	<ul style="list-style-type: none"> <li>• Set up procedures within Austria that will ensure freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles).</li> <li>• Modify the OeNB regulations adopted pursuant to the DevG in order to make possible freezing of funds and assets held by EU-internals in all instances set forth by SR.III.</li> <li>• Provide more guidance to the private sector, especially the non banking financial industry and DNFBPs, on the freezing obligations stemming from the international standard.</li> </ul>
2.5 The Financial Intelligence Unit and its functions (R.26, 30 and 32)	<ul style="list-style-type: none"> <li>• Review the legal framework in order to clearly establish a Financial Intelligence Unit that serves as a national center for receiving, analyzing and disseminating disclosures of STRs and other relevant information concerning suspected ML or FT activities.</li> <li>• Empower this FIU to analyze STRs, prior to any police or criminal investigation, with access to the financial, administrative and law enforcement information and authorization to obtain additional information from reporting parties.</li> </ul>
2.6 Law enforcement, prosecution and other competent authorities (R.27, 28, 30 and 32)	<ul style="list-style-type: none"> <li>• Soften the requirements for law enforcement authorities to obtain access to information held by financial institutions and by lawyers and notaries.</li> </ul>
2.7 Cross Border Declaration and Disclosure (SR.IX)	<ul style="list-style-type: none"> <li>• Subject to disclosure or declaration obligations the transportation of cash or other bearer negotiable instruments into/out of the municipalities of Jungholz and Mittelberg.</li> <li>• Develop a computerized database for the storage of the information gathered through the declaration/disclosure process which should be used to build up intelligence to target cash couriers and to fight against ML/FT.</li> <li>• Assess the risk and develop a strategy for containing the ML/FT risk associated to the transportation of cash or other bearer negotiable instruments into/out the municipalities of Jungholz and Mittelberg.</li> <li>• Enhance cooperation between the customs and the A-FIU and develop a system to enhance the reporting of cases of cross-border transportation to the A-FIU.</li> </ul>
<b>3. Preventive Measures– Financial Institutions</b>	
3.1 Risk of money laundering or	

terrorist financing	
3.2 Customer due diligence, including enhanced or reduced measures (R.5–8)	<ul style="list-style-type: none"> <li>• Require that holders of savings documents for savings deposit accounts which balance is lower than EUR 15,000 and are not registered in the customer’s name, be considered as beneficial owners and be subject to corresponding identification and verification obligations.</li> <li>• Extend CDD measures to customers that are credit and financial institutions established in EU member countries.</li> <li>• Remove the blanket exemption for fiduciary accounts below EUR 15,000.</li> <li>• Conduct ML/FT risk assessment and require enhanced due diligence measures with respect to business relationships and transactions that are of higher risk.</li> <li>• Issue guidelines on the extent of the CDD measures on a risk sensitive basis.</li> <li>• Request financial institutions to apply enhanced due diligence when a customer becomes a PEP after the establishment of the business relationship.</li> <li>• Introduce an explicit requirement that the enhanced due diligence requirements should apply in the event that a PEP is the beneficial owner.</li> <li>• Apply the measures listed under Article 40b, paragraph 1, no. 2 of the BWG to all correspondent banking, that is, also with respect to EEA Member States.</li> <li>• Require financial institutions to have policies in place or to take measures to prevent the misuse of technological developments in ML/FT schemes.</li> <li>• Consider requiring banks to remove the fee charged for closing a savings deposit account.</li> </ul>
3.3 Third parties and introduced business (R.9)	The authorities should determine whether EU and EEA countries where third parties are based adequately apply the FATF Recommendations.
3.4 Financial institution secrecy or confidentiality (R.4)	<ul style="list-style-type: none"> <li>• Lighten the conditions set out in Article 116 of the StPO for disclosure of banking information in order to facilitate access by the police to banking records.</li> </ul>
3.5 Record keeping and wire transfer rules (R.10 and SR.VII)	<ul style="list-style-type: none"> <li>• The recommendations are fully observed.</li> </ul>
3.6 Monitoring of transactions and relationships (R.11 and 21)	<ul style="list-style-type: none"> <li>• For insurance undertakings, extend the requirement to</li> </ul>

	<p>monitor transactions to all unusual patterns of transactions.</p> <ul style="list-style-type: none"> <li>• Define in law, regulation or other enforceable means a requirement for financial institutions to examine the background and purpose of all complex, unusual large transactions, or patterns of transactions, that have no apparent or visible economic or lawful purpose, and to keep resulting findings for at least five years.</li> <li>• Define in law, regulation or other enforceable means a requirement for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations, to examine the background and the purpose of those transactions which have no apparent economic or visible lawful purpose and to keep written findings.</li> </ul>
<p>3.7 Suspicious transaction reports and other reporting (R.13, 14, 19, 25, and SR.IV)</p>	<ul style="list-style-type: none"> <li>• Extend financial institutions' requirement to report to the A-FIU in order to cover all situations when there is a suspicion that funds are the proceeds of a criminal activity, and not only when there is a suspicion that a transaction serves the purpose of money laundering.</li> <li>• Apply the obligation to make a STR to funds that are the proceeds of piracy and counterfeiting, and require professions under the GewO to report STRs in case of self-laundering.</li> <li>• Supervisors should issue guidance to clarify that the reporting obligations extend to situations where persons are suspected of being a terrorist or belonging to a terrorist organization.</li> <li>• As noted in the discussion of SR II, authorities should clarify and strengthen criminal law requirements concerning liability for financing individual terrorists and terrorist organizations.</li> <li>• Increase effectiveness of the reporting system and mitigate the current self-limitation of reporting entities due to the criminal procedure rules.</li> <li>• Apply the protection for STR reporting only in case of good faith for insurance intermediaries.</li> <li>• Prohibit a financial institution to refer a customer to the police when a transaction has been suspended following an STR.</li> <li>• Require financial institutions to report transactions suspected of being related to terrorism, to terrorist organizations, or to those who finance terrorism, in situations where there is no</li> </ul>

	<p>link to a terrorist act.</p> <ul style="list-style-type: none"> <li>• Update FMA guidance on reporting.</li> </ul>
<p>3.8 Internal controls, compliance, audit and foreign branches (R.15 and 22)</p>	<ul style="list-style-type: none"> <li>• Establish the compliance officer function as a management position.</li> <li>• Give the AML/CFT compliance officer the right to access CDD data and information, transaction records and other relevant information.</li> <li>• Integrate AML/CFT compliance into internal audit work, notably for securities and insurance businesses.</li> <li>• Conduct adequate staff screening.</li> <li>• Extend in laws, regulations or other enforceable means the obligation to apply provisions consistent with home country requirements and the FATF Recommendations to all AML/CFT requirements.</li> <li>• Require domestic financial institutions to maintain an internal audit function.</li> </ul>
<p>3.9 Shell banks (R.18)</p>	<p>The recommendation is fully observed.</p>
<p>3.10 The supervisory and oversight system—competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 30, 29, 17, 25, and 32)</p>	<ul style="list-style-type: none"> <li>• Make sanctions sufficiently proportionate and dissuasive.</li> <li>• Extend sanctions under administrative criminal procedure to supervisory board and senior management members.</li> <li>• Ensure that capital held in form of bearer shares does not undermine the assessment of significant or controlling interest in a financial institution.</li> <li>• Carry out fit and proper tests of senior managers and supervisory board members.</li> <li>• Increase onsite examinations on AML/CFT compliance, as well as supervisory oversight of standards within branches and subsidiaries located abroad.</li> <li>• Ensure that licensing requirements or other legal or regulatory measures would prevent criminals to control domestic financial institutions, and apply fit and proper test for their directors and senior managers.</li> <li>• Develop additional guidance available to industry on the new legal requirements.</li> <li>• Establish a regime of supervisory sanctions for domestic financial institutions.</li> <li>• Provide resources, training and support sufficient to enable</li> </ul>

	supervisory divisions to increase AML/CFT oversight.
3.11 Money value transfer services (SR.VI)	<ul style="list-style-type: none"> <li>• Revise the framework for preventive measures to address all deficiencies.</li> </ul>
<b>4. Preventive Measures– Nonfinancial Businesses and Professions</b>	
4.1 Customer due diligence and record-keeping (R.12)	<p><u>All DNFBPs</u></p> <ul style="list-style-type: none"> <li>• Review the requirements concerning PEPs.</li> </ul> <p><u>Casinos</u></p> <ul style="list-style-type: none"> <li>• Extend the legal framework in order to cover all casinos operating in Austria.</li> <li>• Establish legal requirements of CDD for internet casinos.</li> <li>• Establish rules to determine the basis upon which internet casinos are subject to AML/CFT requirements.</li> <li>• Set out a legal obligation for casinos to perform CDD for all customers, including non EU/EEA citizens, when they engage in financial transactions equal to or above EUR 3,000.</li> <li>• Require casinos to perform specific review for higher risk categories and enhanced due diligence for higher risk customers, such as non-resident customers.</li> <li>• Require casinos to put in place appropriate management systems to determine whether a potential customer, a customer or the beneficial owner is a PEP.</li> <li>• Set out enforceable requirements for Internet casinos in order to address the specific risks related to non-face-to-face transactions.</li> <li>• Require casinos to keep record of transactions.</li> </ul> <p><u>Real estate agents, dealers in precious stones and metals, and TCSPs</u></p> <ul style="list-style-type: none"> <li>• Effectively implement GewO requirements regarding TCSP activities; review the Chamber of commerce’s business profiles of management consultant, office work (<i>Büroarbeiten</i>), and office services (<i>Büroservice</i>).</li> <li>• Require to verify that any person purporting to act on behalf of the customer is so authorized.</li> <li>• Absence of guidelines issued by competent authorities to determine the extent of the CDD measures on a risk sensitive</li> </ul>

	<p>basis;</p> <ul style="list-style-type: none"> <li>• Require to perform specific review for higher risk categories and enhanced due diligence for higher risk customers, such as non-resident customers.</li> <li>• Review the framework of simplified CDD measures in line with the standard.</li> <li>• Require to set forth and keep findings of examination of complex and unusual transactions.</li> <li>• Effectively implement the CDD requirements.</li> </ul> <p><u>Lawyers and Notaries</u></p> <ul style="list-style-type: none"> <li>• Clarify the scope of the CDD requirements.</li> <li>• Eliminate the reference to risk in the requirement to identify and verify the beneficial owner.</li> <li>• Require enhanced due diligence for higher risk categories such as non-resident customers or private banking.</li> <li>• Review the framework of simplified CDD measures in line with the standard.</li> <li>• Adopt CDD measures concerning existing customers.</li> <li>• Require lawyers and notaries to pay special attention to all complex and unusual transactions.</li> <li>• Review the disposition regarding the legal privilege in order not to hamper CDD measures.</li> <li>• Issue guidance for lawyers in order to facilitate effective implementation.</li> </ul> <p><u>Accountants</u></p> <ul style="list-style-type: none"> <li>• Clarify the scope of the CDD requirements.</li> <li>• Eliminate the reference to risk in the general CDD requirement.</li> <li>• Eliminate the reference to risk in the requirement to identify and verify the beneficial owner.</li> <li>• Review the framework of simplified CDD measures in line with the standard.</li> <li>• Require to set forth and keep findings of examination of complex and unusual transactions.</li> <li>• Review the disposition regarding the legal privilege in order not to hamper CDD measures.</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>Effectively implement the CDD requirements.</li> </ul>
4.2 Suspicious transaction reporting (R.16)	<p><u>All DNFBPs</u></p> <ul style="list-style-type: none"> <li>Align the grounds for reporting on the standard.</li> <li>Give special attention to business relationships and transactions with persons from countries insufficiently applying the FATF recommendations.</li> </ul> <p><u>Casinos</u></p> <ul style="list-style-type: none"> <li>Require Internet casinos to report STRs and specify AML/CFT internal controls.</li> </ul> <p><u>Real estate agents, dealers and TCSPs</u></p> <ul style="list-style-type: none"> <li>Effectively extend the legal obligation to report STRs and have internal control in place to all businesses and professions conducting TCSP activities.</li> </ul> <p><u>Lawyers and notaries</u></p> <ul style="list-style-type: none"> <li>Consider reviewing the matters that fall under legal professional secrecy of notaries and lawyer, that currently appear very broad.</li> </ul> <p><u>Accountants</u></p> <ul style="list-style-type: none"> <li>Consider reviewing the matters that fall under legal professional secrecy of accountants, which currently appear very broad.</li> </ul>
4.3 Regulation, supervision, monitoring, and sanctions (R.17, 24, and 25)	<ul style="list-style-type: none"> <li>Give the Ministry of Finance adequate powers to perform AML/CFT supervision of internet casinos.</li> <li>Empower the Ministry of Finance to perform controls on the beneficial owners of a significant or controlling interest in casinos, and to prevent actions by associates of criminals.</li> <li>Put in place a system for monitoring and ensuring compliance with AML/CFT requirements to cover accountants and all the companies active in the TCSP sector.</li> <li>Give trade authorities the necessary technical and budgetary resources to perform effectively their functions.</li> <li>Review the amount of the fines permissible under the GewO.</li> <li>Establish guidelines tailored to the specific needs of each DNFBP, as these currently exist only for notaries, and partially for casinos.</li> <li>Provide information on current techniques, methods and trend tailored to each DNFBP, as well as systematic case by case</li> </ul>

	feedback on STRs.
4.4 Other designated non-financial businesses and professions (R.20)	<ul style="list-style-type: none"> <li>• Take additional measures to reduce the relative importance of use of cash and large denomination banknotes.</li> </ul>
<b>5. Legal Persons and Arrangements and Nonprofit Organizations</b>	
5.1 Legal Persons–Access to beneficial ownership and control information (R.33)	<ul style="list-style-type: none"> <li>• Make the regime of private foundations more transparent on beneficial ownership, for example by requiring that the appendix/supplementary declaration be available in the Commercial Register, to reduce the risk that these foundations may be used for ML.</li> <li>• Establish a legal mechanism to trade shares in the Stock exchange in nominative form or adopt legal provisions to make “de-materialization” mandatory.</li> <li>• Conduct an assessment to determine the ML risk potentially associated to the use of bearer shares.</li> </ul>
5.2 Legal Arrangements–Access to beneficial ownership and control information (R.34)	<ul style="list-style-type: none"> <li>• Ensure transparency where the property held in <i>Treuhand</i> is composed of assets other than funds (regardless of the <i>Treuhänder</i>), where the <i>Treuhänder</i> is someone other than a lawyer, notary or registered TSP, where funds held under <i>Treuhand</i> by lawyers amount to less than the federal state threshold (i.e., between EUR 15,000 and EUR 40,000).</li> <li>• Ensure transparency over foreign trusts operated from Austria.</li> <li>• Implement AML/CFT oversight to ensure TSPs properly obtain, verify and record details of the <i>Treuhand</i> and its beneficial ownership.</li> <li>• Develop effective means by which bodies charged with the oversight of TSPs for AML/CFT purposes can share information with their national or foreign counterparts.</li> </ul>
5.3 Nonprofit organizations (SR.VIII)	<ul style="list-style-type: none"> <li>• Require NPOs operating under the legal form of private foundations to make information on the identity of persons who own, control or direct their activities, publicly available.</li> <li>• Strengthen requirements for NPOs to maintain and make available to appropriate authorities records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organization.</li> <li>• Strengthen outreach to the NPO sector.</li> </ul>

<b>6. National and International Cooperation</b>	
6.1 National cooperation and coordination (R.31 and 32)	The recommendations are fully observed.
6.2 The Conventions and UN Special Resolutions (R.35 and SR.I)	<ul style="list-style-type: none"> <li>• Criminalize self-laundering.</li> <li>• Soften the requirements for law enforcement authorities to obtain access to information subject to secrecy.</li> <li>• Extend the criminalization to the whole range of activities envisaged by Article 2, paragraphs 5(b) and (c) of the 1999 UN Convention.</li> <li>• Set up procedures within Austria that will ensure freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles).</li> <li>• Modify the OeNB regulations adopted pursuant to the Exchange of Control Act (for EU-internal terrorists) in order to make possible freezing of funds and assets held by EU-internals in all instances set forth by UNSCR 1373 and SR.III.</li> </ul>
6.3 Mutual Legal Assistance (R.36, 37, 38, SR.V and 32)	<ul style="list-style-type: none"> <li>• Ensure that MLA is granted in a timely, constructive and effective manner.</li> <li>• Conclude arrangements for coordinating seizure and confiscation actions with other countries.</li> <li>• Remove from banking secrecy provisions all requirements which may hinder effective cooperation.</li> <li>• Ensure that extensive scope of legal privilege does not slow down effective cooperation.</li> <li>• Consider sharing of confiscated assets with countries other than EU members and the United States.</li> </ul>
6.4 Extradition (R. 39, 37, SR.V and R.32)	<ul style="list-style-type: none"> <li>• Take steps to improve the overall effectiveness of the extradition framework.</li> </ul>
6.5 Other Forms of Cooperation (R. 40, SR.V and R.32)	<ul style="list-style-type: none"> <li>• Grant the A-FIU the sufficient resources in order to respond to foreign FIU requests in a timely way.</li> <li>• Enable the A-FIU to exchange information on FT.</li> <li>• Establish provisions which allow competent authorities to conduct inquiries on behalf of securities supervisors from third countries.</li> </ul>
<b>7. Other Issues</b>	

7.1 Resources and statistics (R. 31 and 32)	<ul style="list-style-type: none"><li>• Improve the statistical apparatus.</li><li>• Provide for additional resources for the police and supervisory bodies.</li></ul>
7.2 Other relevant AML/CFT measures or issues	
7.3 General framework – structural issues	

**Annex 1. Authorities' Response to the Assessment**

The authorities chose not to respond to the assessment.

**Annex 2. Details of All Bodies Met During the On-Site Visit****Federal and Local Authorities**

Federal Ministry of Economy, Family and Youth (MoE)  
Federal Ministry for European and International Affairs (MoFA)  
Federal Ministry of Finance (MoF)  
Federal Ministry of Justice (MoJ)  
Federal Ministry of the Interior (MoI)  
State Authorities

**Criminal Justice and Operational Agencies**

Austrian Financial Investigation Unit (A-FIU)  
Criminal Intelligence Service (BKA)  
Federal Agency for State Protection and Counter-Terrorism (BVT)  
Judges and Public Prosecutors

**Financial Sector Supervisory Bodies**

Austrian National Bank (OeNB)  
Financial Market Authority (FMA)

**Private Sector Bodies**

Austrian Chamber of Notaries (ÖNK)  
Austrian Federal Economic Chamber (WKO)  
Austrian Insurance Association (VVO)  
Bar Association  
Chamber of Chartered Accountants (KWT)  
Parity Commission for Accounting Professions

**Private Sector Representatives**

Academics  
Accountants  
Audit firms  
Casinos  
Credit and domestic financial institutions  
Dealer in precious metals and stones  
Insurance undertakings  
Investment firms  
Lawyers  
Notaries

### Annex 3. List of All Laws, Regulations, and Other Material Received

- Agreement between Austria-Hungary and the German Empire from 2 December 1890 concerning the accession of the borough of Mittelberg in Vorarlberg to the German customs union
- Agreement from 3 May 1868 between His Imperial and Royal Apostolic Majesty and His Majesty the King of Bavaria, concerning the accession of the borough of Jungholz, which belongs to the county of Tyrol, to the Bavarian customs and indirect tax system
- Associations Act (*Vereinsgesetz, VerG*)
- Austrian Police Cooperation Act (extracts)
- Banking Act (*Bankwesengesetz, BWG*)
- Code of Criminal Procedure (*Strafprozessordnung, StPO*) (extracts)
- Commercial Code (*Unternehmensgesetzbuch, UGB*) (extracts)
- Commission Communication NPO COM(2005)620
- Council Common Position 2001/930/CFSP of 27 December 2001 on combating terrorism
- Council Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism
- Council Common Position 2002/402 CFSP of 27 May 2002 concerning restrictive measures against Usama bin Laden, members of the Al-Qaida organization and the Taliban and other individuals, groups, undertakings and entities associated with them and repealing Common Positions 96/746/CFSP, 1999/727/CFSP, 2001/154/CFSP and 2001/771/CFSP
- Council Common Position 2003/140/CFSP of 27 February 2003 concerning exceptions to the restrictive measures imposed by Common Position 2002/402/CFSP Council Common Positions 96/746/CFSP, 1999/727/CFSP, 2001/154/CFSP and 2001/771/CFSP
- Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information
- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence
- Criminal Code (*Strafgesetzbuch, StGB*) (extracts)
- Criminal Intelligence Service Act (*Bundeskriminalamtgesetz, BKA-G*) (extracts)
- Customs Law (*Zollrechts-Durchführungsgesetz, ZollR-DG*) (extracts)
- Decision of the Supreme Administrative Court of 11 March 2008 (GZ AW 2008/17/0004) (extracts)
- Decree of 11 November 2008 on the relationship between reporting obligations and the transaction ban under §41 Austrian Banking Act (BWG) and criminal proceedings; witness protection
- Directive 2002/92/EC of 9 December 2002 on insurance mediation
- Directive on the Practice of the Accountancy Professions (*Bilanzbuchhaltungs-(Berufs) Ausübungsrichtlinie, BiBu-ARL*)
- Directive on the Practice of the Chartered Public Accountants and Tax Consultants Professions (*WirtschaftsTreuhandberufs-Ausübungsrichtlinie, WT-ARL*) (extracts)
- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005, on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC
- Europol Convention
- Explanatory Notes to the RAO, NO, GewO and BWG (extracts)
- Federal Constitutional Law (*Bundes-Verfassungsgesetz, B-VG*) (extracts)
- Federal law on judicial cooperation in criminal matters with the Member States of the European Union (*Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union, EU-JZG*)

- Financial Market Authority Act (*Finanzmarktaufsichtsbehördengesetz, FMABG*)
- FMA Circular: Control Procedures and STRs (Banks) (2004); Identification (Insurances) (2006) Identification and Verification of Identity (Banks) (2008); *Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen* (13.11.2008)
- Fiscal Penal Code (*Finanzstrafgesetz, FinStrG*) (extracts)
- Foreign Exchange Act (*Devisengesetz, DevG*)
- Gambling Law (*Glücksspielgesetz, GSpG*)
- Guidelines by the Austrian Chamber of Civil-Law Notaries on Procedures Governing Notarial Trusteeships of 8 June 1999 (extracts)
- Insurance Supervision Act (*Versicherungsaufsichtsgesetz, VAG*)
- Law on Extradition and Mutual Assistance (*Auslieferungs- und Rechtshilfegesetz, ARHG*) extracts
- Lawyer's Act (*Rechtsanwaltsordnung, RAO*)
- Notaries' Act (*Auszug aus der Notariatsordnung, NO*) (extracts)
- Oberste Gerichtshof 1Ob57/04w and 1Ob40/04w (both in German)
- Official Announcement DL 1/2008 of the OeNB according to Art 4 of the DevG
- Police Cooperation Act (*Polizeikooperationengesetz, PolKG*)
- Recommendations by the Austrian Chamber of Civil Law Notaries on the Prevention of Money Laundering/Terrorist Financing (status January 2009)
- Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter the Commission to ensure the correct application of the law on customs and agricultural matters
- Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism
- Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with *Usama bin Laden*, the *Al-Qaida* network and the *Taliban*, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the *Taliban* of Afghanistan
- Regulation (EC) No 561/2003 of 27 March 2003 amending, as regards exceptions to the freezing of funds and economic resources, Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with *Usama bin Laden*, the *Al-Qaida* network and the *Taliban*
- Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community
- Regulation (EC) 1781/2006 of the European Parliament and of the Council of 15 November 2006 on Information on the Payer Accompanying Transfers of Funds
- Regulation on the Annex to the Audit Report on the Annual Financial Statements (BGBl. II Nr. 310/2008)
- Securities Supervision Act (*Wertpapieraufsichtsgesetz, WAG*)
- Security Police Act (*Sicherheitspolizeigesetz, SPG*)
- Statute on the Responsibility of Entities for Criminal Offenses (*Verbandsverantwortlichkeitsgesetz VbVG*)
- Stock Exchange Law (*Börsegesetz, BörseG*)
- Trade Act (*Gewerbeordnung, GewO*) (extracts)

**Annex 4. Copies of Key Laws, Regulations, and Other Measures**

StGB, Criminal Code

StPO, Code of Criminal Procedure

ARHG, Law on Extradition and Mutual Assistance

EU-JZG, Law on Judicial Cooperation in Criminal Matters with EU Member State

PolK, Police Cooperation Act

SPG, Security Police Act

BWG, Banking Act

VAG, Insurance Supervision Act

FMABG, Financial Market Authority Act

Trade Act, GewO

## **StGB (Criminal Code)**

### **Extracts**

#### **Art. 12 (Treatment of all Participants as offenders)**

A criminal offence is committed not only by the immediate perpetrator that commits the criminal offence but also by anybody who abets another person to commit the offence or who contributes to its perpetration in any other way.

#### **Art. 15 (Punishability of attempt)**

(1) Punitive sanctions against offences committed intentionally do not only apply to the completed offence but also to its attempt and any participation in an attempt.

(2) An offence is considered attempted as soon as the offender puts his decision to commit the offence or have another person commit it (§ 12) into practice by taking an action immediately preceding the commission of the offence.

(3) An attempted offence and participation in an offence will not be liable to punishment if the offence could not have been completed under any circumstances for lack of the perpetrator's personal qualities or circumstances required under the law, or on account of the type of action or object that has been subject to the offence.

#### **Art. 17 (graduation of criminal offences)**

(1) Crimes are intentional acts liable to a life sentence or to imprisonment of more than 3 years.

(2) All other criminal offences are regarded as misdemeanours.

1 Federal Law Gazette 1974/60 last amended by Federal Law Gazette I No. 109/2007

2 square bracket terms refer to the last amendment (BGBl = Federal Law Gazette)

#### **Art. 20 (Confiscation of Profits)**

(1) Whoever

1. has committed an offence and has obtained economic benefit from it, or
2. has received economic benefit for committing an offence,

is to be condemned to payment of an amount of money equivalent to the gained illegal profits. Insofar as the extent of the profits cannot be established at all, or cannot be established without disproportionate expenditure, the court may fix the sum of money to be confiscated according to its conviction.

(2) If the perpetrator

1. has committed crimes (sect. 17) continuously or repeatedly and has obtained economic benefits from, or received for, their commission and
2. has gained during the same period further economic benefits, there being an obvious supposition that these benefits derive from other crimes of the same nature, and the legal acquisition of the benefits not being made credible,

these economic benefits have to be taken into consideration in fixing the amount of money to be confiscated.

(3) A perpetrator who, during the period of his membership in a criminal organization (sect. 278a) or in a terrorist group (sect. 278b), has gained economic benefits, is to be condemned to payment of an amount of money the court may fix corresponding to the gained profits according to its conviction, if there is an obvious supposition that these profits derive from offences and their legal acquisition cannot be made credible.

(4) Whoever profits illegally and directly from an offence committed by another person, or from the economic benefit given for the commission of such an offence, is to be condemned to payment of an amount of money equivalent to these profits. This applies *mutatis mutandis* to legal persons and partnerships which have gained profits.

(5) If the person who has gained illegal profits has died, or if the legal person or partnership has ceased to exist, the profits are to be confiscated from the legal successor insofar as they were still existent at the moment of transmission of rights.

(6) A majority of persons who have gained illegal profits are to be condemned according to their respective shares. If the share cannot be established, the court has to fix it according to its conviction.

#### **Art. 20a (Abstention from the Confiscation of Profits)**

(1) The confiscation of profits is excluded insofar as the person who has gained illegal profits has satisfied civil claims derived from the criminal act or has undergone the contractual and enforceable obligation to do so, or has been condemned, or is condemned simultaneously, to do so or if and insofar as the profits are removed by other legal measures.

(2) It is to be refrained from the confiscation of profits

1. *[abolished]*

2. insofar as the amount of money to be confiscated or the chances to enforce the order is disproportionate to the expenditure for proceeding to such order or for its enforcement, or

3. insofar as the payment of the amount of money would unreasonably endanger the subsistence of the person who has gained the profits or would constitute an inappropriate hardship for him, especially because the profits do not exist any more at the time of the order; other disadvantageous consequences of a conviction are to be taken into consideration.

#### **Art. 20b (Forfeiture)**

(1) Property being at the disposal of a criminal organization (sect. 278a) or a terrorist group (Sect. 278b) or which has been provided or collected as a means for financing terrorism shall be declared forfeited.

(2) Property deriving from an offence where Austrian jurisdiction is not established under sect. 62 to 65 shall be declared forfeited if the offence is punishable under the law of the State where it was committed.

#### **Art. 20c (Abstention from Forfeiture)**

(1) Forfeiture is excluded insofar as

1. the property concerned is legitimately claimed by a person not having participated in the offence or in the criminal organization or terrorist association, or

2. its purpose is achieved by other legal measures, especially insofar as the illegal profits are declared confiscated in foreign proceedings and if the foreign decision can be executed in Austria.

(2) Forfeiture is to be refrained from if it would be out of proportion to the importance of the matter, or to the expenditure implied.

#### **Art. 165 (Money laundering)**

(1) Whoever conceals property items that derive from the crime of another person, from such an offence under sections 168c, 168d, 223, 224, 225, 229, 230, 269, 278, 278d, 288, 289, 293, 295 or 304 to 308, or from such a tax offence of smuggling or evasion of import or export taxes (insofar as these fall within the competence of the courts), or disguises the origin thereof, particularly by giving in legal relations false information regarding the origin or true nature of those property items, the ownership of or other rights to them, the right to dispose of

them, their transfer or their location, shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding 360 daily rates.

(2) Whoever knowingly acquires such property items, holds them in custody, invests, administers, converts, realizes, or transfers them to a third party, shall be liable in the same way.

(3) Whoever commits the offence involving items worth more than 50,000 Euro or as the member of a criminal group associated for the purpose of continuous money laundering shall be liable to imprisonment for a term of six months to five years.

(4) A property item shall be deemed to derive from an offence when the perpetrator of the crime has obtained it through that offence or received it for the commission of that offence, or when it represents the value of the originally obtained or received property item.

(5) Whoever knowingly, acting on behalf or in the interest of a criminal organization (sect. 278a) or of a terrorist group (sect. 278b), acquires property items of that organization or group, holds them in custody, invests, administers, converts, realizes, or transfers them to a third party, shall be liable to imprisonment for a term not exceeding three years; whoever commits the offence involving items worth more than 50,000 Euro, to imprisonment for a term from six months to five years.

#### **Art. 278 (Criminal association)**

(1) A person who founds a criminal association or participates in such an association as member is to be sentenced to imprisonment up to three years.

(2) A criminal association is an union planned for a longer time of more than two persons aiming the commitment of one or more crimes by one or more members of the association, other considerable acts of violence against life and limb, not only petty damages to property, thefts or frauds or misdemeanours under sects. 104a, 165, 177b, 233 to 239, 241a to 241c, 241e, 241f, 304 or 307 or under Sect 114 para 2 or 116 Aliens' Police Act.

(3) As member participates in a criminal association who commits a criminal offence within the scope of its criminal orientation or participates in its activities by providing for information or assets or in another way with the awareness that he promotes thereby the association or its criminal acts.

(4) If the association did not lead to a criminal offence in the planned way no member shall be punished if the association dissolves itself voluntarily or it results from its conduct that it has given up its plan voluntarily. Furthermore a person shall not be punished for criminal association who withdraws voluntarily from the association before an offence in the planned way has been committed or attempted; but a person who participated in the association in a leading position only in case he effects by an information of the authority (sect.151 para. 3) or in another way that the danger is removed which arises from the association.

#### **Art. 278a (Criminal organisation)**

Whoever establishes an association of a considerable number of persons, intended to last a longer period of time and similar to an enterprise, or who participates in such an association as a member (sect. 278 para. 3), shall be liable to imprisonment for a term of six months to five years if the association

1. is oriented, even if not exclusively, towards the repeated and planned commission of grave offences against life and limb, freedom, or property, or of grave offences relating to the sexual exploitation of human beings, smuggling of aliens, illegal trafficking in military weapons, nuclear and radioactive material, dangerous waste, counterfeit money or drugs, and

2. aims at profits on a high scale or at considerable influence on politics or economy and

3. undertakes to corrupt, or intimidate, others, or to particularly screen itself against prosecution measures.

Section 278, para. 4, shall apply mutatis mutandis.

**Art. 278b (Terrorist association)**

(1) A person who leads a terrorist association (para. 3) is to be sentenced to imprisonment from five to fifteen years. A person who leads a terrorist association which confines itself to threaten with terrorist offences (sect. 278c para. 1) is to be sentenced to imprisonment from one year to ten years.

(2) A person who participates in a terrorist association as member (sect. 278 para. 3) is to be sentenced to imprisonment from one year to ten years.

(3) A terrorist association is an union planned for a longer time of more than two persons aiming the commitment of one or more terrorist criminal offences (sect. 278c) by one or more members of the association.

**Art. 278c (Terrorist criminal offences)**

(1) Terrorist criminal offences are

1. murder (sect.75),
2. bodily injuries under sections 84 to 87,
3. extortionate kidnapping (sect. 102),
4. gross intimidation (sect. 106),
5. dangerous threat (sect. 107 para.2),
6. gross damage to property (sect. 126) and damaging of data (sect. 126a) if thereby a danger to the life of another person or a danger to the property of another person to a large extent can be caused,
7. intentional offences of dangerousness to public safety (sects. 169, 171, 173, 175, 176, 177a, 177b, 178) or intentional infringement of environment (sect. 180),
8. hijacking (sect. 185),
9. intentional danger to the safety of aviation (sect. 186) or
10. a criminal offence punishable under section 50 of the Weapons Act 1996 or section 7 of the War Material Act, if the offence is appropriate to cause a severe interference with the public life or such an interference for a longer time or to cause a severe damage to the economic life being committed with the intent to intimidate the people in a serious manner or to force public authorities or an international organization to an action, permission or omission or to convulse or destroy the politic, constitutional, economic or social basic structures of a state or an international organization.

(2) A person who commits a criminal offence under para. 1 shall be punished pursuant to the law applicable to the offence mentioned there, and the maximum penalty is to be increased by half of the penalty being prescribed respectively, but not exceeding twenty years.

(3) The offence is not regarded as terrorist criminal offence if it is directed to the establishment or re-establishment of a democratic and constitutional situation or the exercise or observance of human rights.

**Art. 278d (Financing of terrorism)**

(1) A person who provides for assets of property or collects them with the intent that they are used for the commitment

1. of a hijacking (sect. 185) or an intentional danger to the safety of aviation (sect. 186),
2. of an extortionate kidnapping (sect. 102), or the threat with it,
3. of an attack on life and limb or the freedom of a person protected by international law or a violent attack on an apartment, the official premises or the means of transportation of such a person which is appropriate to expose this person to a danger to life and limb or freedom or a threat with it;

4. of an intentional endangering by nuclear energy or ionized radiation (sect. 171) or a threat with it, of a unlawful use of nuclear materials or radioactive substances (sect. 177b), of any other criminal offence to obtain nuclear materials or radioactive substances or of the threat to commit a theft or robbery of nuclear materials or radioactive substances aiming to force another person to an action, permission or omission;
  5. of a considerable attack on life and limb of another person on an airport serving the international civil aviation, of an destruction or considerable damaging of such an airport or a civil aircraft being on it or an interruption of the services on the airport, so far as the offence is committed by the use of a weapon or other device and is appropriate to endanger the security of the airport;
  6. of a criminal offence committed in a way mentioned in sects. 185 or 186 against a vessel or a fixed platform, against a person being on board of a vessel or a fixed platform or against the cargo loaded on a ship or an equipment of the ship;
  7. of the transportation of a blasting composition or another deadly device in a public place, to a governmental or public institution or a public traffic system or services of supply or of the operation of these means aiming to cause the death or a grievous bodily injury of another person or the destruction of the place, institution or system to a high degree, as far as the destruction is appropriate to bring about a considerable economic damage;
  8. of a criminal offence which shall effect the death or a grievous bodily injury of a civil person or another person not being actively involved in the hostilities of an armed conflict if this act is aimed for the reason of its nature and the circumstances at threatening a group of the population or forcing a government or an international organization to an action or omission; is to be sentenced to imprisonment from six months to five years. But the nature and extent of the sentence must not be severer than the penalty provided for the financed offence.
- (2) The offender shall not be punished under para. 1 if the offence is subject to a severer penalty under another provision.

**StPO (Code of Criminal Procedure)**

**Extracts**

**CHAPTER 8: Investigation measures and taking of evidence**

**Part 1: Seizure, sequestration and information on bank accounts and bank operations**

**Definitions**

**Section 109.**

For the purpose of this law

1. “seizure” shall mean the temporary constitution of the authority to dispose over objects and the temporary prohibition to hand over object or other assets to third persons (third party prohibition) and the temporary prohibition to alienate or pledge such objects and assets,
2. “sequestration” shall mean a decision of a court to constitute or continue a seizure in terms of n° 1 and the prohibition by a court to alienate, encumber or pledge real estates or rights listed in a public register,
3. “information on bank accounts and bank operations” shall mean the disclosure of the name and other information about the identity of the holder of a business relation as well as his/her address and the information whether an accused person maintains business relations with this institution, is entitled to economic advantages from this relation or authorised by such relation as well as the presentation of all documents regarding the identity of the holder of the business relation and his authorisation to act, access to documents and other papers of a credit or financial institution regarding the nature and extend of a business relation and other business operations for a determined past or future period of time.

**Seizure**

**Section 110.**

(1) A seizure can be admitted if it is considered necessary

1. due to reasons of evidence,
2. for securing rights based in civil law (section 367) or
3. for securing the confiscation of proceeds of crime (section 20 StGB [*Österreichisches Strafgesetzbuch-Austrian Criminal Code*], the forfeiture (section 20b StGB), the confiscation (section 26 StGB) or another order relating to property rights provided for in the law.

(2) The seizure is to be ordered by the office of public prosecution and executed by the criminal police.

(3) The criminal police is entitled to seize objects at their own discretion (section 109 n° 1 lit. a)

1. if they are under nobody’s authority to dispose, have been taken from a victim of a criminal act, have been found on the crime scene and could have been used or determined to be used for committing the criminal act, or are of low value or can be easily substituted for a limited period of time,
2. if their possession is generally prohibited (section 445a para. 1),
3. that are in the possession of a person arrested for reasons of section 170 para. 1 n° 1 when arrested or that are found during a search according section 120 para. 1, or
4. in the cases of article 4 of the Council Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights (*Official Journal L 196, 02/08/2003 P. 0007 – 0014*).

(4) The seizure of objects due to reasons of evidence (para. 1 n° 1) is not admitted and in any case has to be terminated if the affected person requests it, if and as soon as the aim of the evidence can be met with picture, sound or other recordings or with copies of written documents or data processed automation-aided and if there is no reason to assume that the seized objects themselves or the original versions of the information seized will have to be inspected during the court proceeding.

#### **Section 111.**

(1) Every person who possesses objects or assets to be seized is obliged (section 93 para.2) to hand them over to the criminal police if requested so or to ensure the seizure in any other way. This obligation can be executed by force if necessary by searching the persons or domiciles. In this case sections 119 to 122 are to be applied analogously.

(2) If information stored on data carriers is to be seized anyone has to grant access to this information and on request hand over or produce an electronic data storage medium in a file format commonly used. Moreover he/she has to abide the creation of a backup copy of the data stored on the data storage medium.

(3) To persons that are not accused of the criminal act themselves the appropriate and common costs necessarily incurred to them by the separation of documents or other objects of evidence from other things or by handing over copies have to be refunded on their application.

(4) In any case the person affected by the seizure has to be given or served a confirmation of the seizure immediately or at the latest within 24 hours that also informs them about their right to object (section 106). In case of a seizure in order to secure civil rights claims (section 110 para. 1 n° 2) the victim has to be informed if this is possible.

#### **Section 112.**

If the person affected by the seizure or a person present at the seizure contests to the seizure of written documents or data carriers referring to an obligation to maintain secrecy recognised by law, these documents or data carriers have to be secured against any form of inspection without permission or against any alteration and have to be presented to the court. They must not be inspected before this. The court has to inspect the documents and the data carriers and to decide whether and to what extent they have to be seized or given back to the affected person. A complaint against this decision has suspensory effect.

#### **Section 113.**

(1) The seizure terminates

1. if the criminal police sets it aside (para. 2)
2. if the office of public prosecution orders the cancellation (para. 3),
3. if the court orders the sequestration.

(2) The criminal police has to report to the office of public prosecution immediately but at the latest within 14 days of any seizure (section 100 para. 2 n° 2), unless the seizure is set aside according to section 110 para. 3 earlier on the grounds that the prerequisites are not or no longer fulfilled. This report can be combined with the following report if this is not detrimental to the interests of the case or of persons and if the seized objects are of low value, are under nobody's authority to dispose or their possession is generally prohibited (section 445a para. 1). In the case of section 110 para. 3 n° 5 the criminal police has to proceed in accordance with the provisions of sections 3, 4 and 6 of the Product Piracy Act 2004 (*Produktpirateriegesetz 2004*), Federal Law Bulletin I N° 56/2004.

(3) The office of public prosecution immediately has to request the court to sequester the objects or, if the prerequisites are not or no longer fulfilled, order the cancellation of the seizure.

#### **Section 114.**

(1) The criminal police is responsible for the custody of the seized objects until the courts decides about the sequestration (section 115 para. 2), after that the office of public prosecution is responsible.

(2) If the reason for continuing the custody of seized objects no longer exists, the objects immediately have to be handed over to the persons in whose disposition they were at the time of the seizure, unless these persons are apparently not entitled to that. In this case the objects have to be handed over to the entitled person or, in case such a person has not been found or can only be found with disproportional effort, they have to be deposited according to section 1425 of the Austrian Civil Code (*Allgemeines Bürgerliches Gesetzbuch-ABGB*). The persons affected by this have to be notified.

### **Sequestration**

#### **Section 115.**

(1) The sequestration is admitted if the objects seized presumably

1. are required as evidence in the following proceeding,
2. are subject to civil law claims (section 367) or
3. will be needed to ensure a judicial decision on the confiscation of proceeds of crime (section 20 StGB), on forfeiture (section 20b StGB), on confiscation (section 26 StGB) or another legally provided measure relating to property rights, whose execution would otherwise be endangered or considerably more difficult.

(2) On request of the office of public prosecution the court has to decide immediately about the sequestration.

(3) Section 110 para. 4 is to be applied analogously. If necessary the sequestration has to be limited to the recordings and copies mentioned there.

(4) For a sequestration via “third party prohibition” and a prohibition to alienate or encumber (section 109 n° 2 lit. b) the provisions of the Austrian Code of Enforcement (*Exekutionsordnung-EO*) on the preliminary injunction are applicable analogously unless this law provides otherwise.

(5) In a decision permitting a sequestration in order to secure a judicial decision on the confiscation of proceeds of crime (section 20 StGB) or forfeiture (section 20b StGB) an amount of money that will cover the presumable confiscation of proceeds of crime or the presumable forfeiture has to be determined.

(6) If and as soon as the prerequisites for the sequestration do not or no longer exist or an amount of money mentioned in para. 5 is deposited, the office of public prosecution, after bringing the writ of accusation the court, has to terminate the sequestration.

### **Information on bank accounts and bank operations**

#### **Section 116.**

(1) The disclosure of information on bank accounts and bank operations is admitted if it seems to be necessary to clarify a criminal offence or misdemeanour under the jurisdiction of the Regional Courts (section 31 para. 2 to 4).

(2) The disclosure of information on bank accounts and bank operations according to section 109 n° 3 lit. b is moreover only admitted if due to ascertained facts it can be assumed that

1. the business relation of a person with the credit or financial institution is connected to committing a criminal act and either the holder of the account himself/herself is suspected of having committed the act or if it is presumed that a person suspected of having committed the act will operate or has operated a transaction via the account, or
2. the business relation will be used for the transaction of a financial benefit that was gained through criminal acts or gained for them (section 20 StGB) or is subject to the disposition of a criminal

organisation or terrorist organisation or is provided or collected as a means of financing terrorism (section 20b StGB).

(3) The disclosure of information on bank accounts and bank operations has to be ordered by the office of public prosecution on the basis of a judicial admission.

(4) Order and admission of the disclosure of information have to contain:

1. the denomination of the court case and the criminal act it is based on as well as its legal denomination,
2. the credit or financial institution,
3. the designation of the documents to be handed over and the information to be disclosed,
4. the facts that constitute the grounds for the necessity and proportionality (section 5) of the order,
5. in the case of an order according to para. 2 the time frame concerning which the operations are to be disclosed,
6. in the case of an order according to para. 2 the facts that constitute the grounds for the connection between the business relation and the subject of the proceeding.

(5) The order together with the judicial admission has to be served to the credit or financial institution, the accused and the persons entitled by the business relation, as soon as they are known to the office of public prosecution. Service to the accused and to the entitled persons can be postponed as long as otherwise the aim of the proceeding would be endangered. The credit or financial institution has to be informed of this and has to keep the order and all facts and operations in connection with it secret against clients and third parties.

(6) Credit and financial institutions and their employees are obliged to disclose the information, to let the documents and papers be inspected and hand them over. For this an electronic data carrier in a common file format has to be used if for the operation of the business relation automation-aided data processing is used. If the credit or financial institution complains against the judicial admission and does not disclose information or hand over documents, it is to proceed according to section 93 para. 2 and 112 with the difference that the documents have to be presented to the Superior Court (*Oberlandesgericht*). A search of credit or financial institutions always requires an order of the office of public prosecution on the basis of a judicial admission. In case more information is needed or more documents are to be provided for inspection or to be handed over, that are not included in the order and admission (para. 4) a procedure according to section 112 is to be initialised if the credit or financial institution requests it. Sections 110 para. 4 and 111 para. 3 are to be applied.

## **Part II: Establishing the identity, search of places and objects, search of persons, body search and molecular genetic inspection**

### **Definitions**

#### **Section 117.**

For the purpose of this law

1. “establishing the identity” means the investigation and determination of data (section 4 n° 1 of the Data Protection Act 2000 [*Datenschutzgesetz 2000*]) that distinctively characterize a certain person,
2. “search of places and objects” means the searching of premises, rooms, vehicles or containers that are not publicly accessible, domiciles or other places protected by the principle of sanctity of the home, and the objects contained within,
3. “search of a person” means the searching of the clothing of a person and of the objects he/she carries with him/her, the inspection of the naked body of a person,

4. “physical examination” means the searching of body orifices, the taking of blood samples and any other interference with the physical integrity of a person,

5. “molecular genetic inspection” means the determination of those parts of the DNA of a person that serve for the purpose of recognition.

### **Establishing the identity**

#### **Section 118.**

(1) Establishing the identity is admissible if, based on ascertained facts, it can be assumed that a person participates in a criminal act, can provide information on the circumstances of committing the act or has left traces that can help to clarify the case.

(2) The criminal police is authorized to investigate the name, sex, date of birth, place of birth, profession and the address of a person in order to establish his/her identity. The criminal police is also entitled to establish the size of a person, to take photographs, to record his/her voice and to take the imprints of his/her friction ridges as far as this is necessary to establish the identity.

(3) Everyone is obliged to cooperate in the establishment of his/her identity in a way appropriate according to the circumstances. If a person requests it, the criminal police has to inform him/her about the reason for establishing his/her identity.

(4) If the person does not cooperate in the establishment of his/her identity or his/her identity due to other reasons cannot be established immediately, the criminal police is entitled to search the person at their own discretion in accordance with section 117 n° 3 lit. a in order to establish the identity.

### **Search of places, objects and persons**

#### **Section 119.**

(1) The search of places and objects (section 117 n° 2) is admissible if, due to ascertained facts, it can be assumed, that a person who is a suspect of a criminal act is hiding there or if there are objects or traces that have to be seized or examined.

(2) The search of a person (section 117 n° 3) is admissible if this person

1. has been arrested or caught in the act,

2. is suspected of committing a criminal act and due to ascertained facts it can be assumed that he/she carries objects that are subject to seizure with him/her or has traces on him/her,

3. has been injured in the criminal act or has been subjected to other physical changes the determination of which is important for the aims of the criminal proceeding.

#### **Section 120.**

(1) The search of places and objects in accordance with section 117 n° 2 lit. b and of persons in accordance with section 117 n° 3 lit. b has to be ordered by the office of public prosecution on the basis of a judicial admission. In cases of imminent danger the criminal police is authorized to conduct these searches provisionally without the order or admission. The same applies in the cases of section 170 para. 1 n° 1 to the search of persons in accordance with section 117 n° 3 lit. b. In no case the victim may be forced to be examined against his/her will (sections 119 para. 2 n° 3 and 121 para. 1 last sentence).

(2) Searches according to section 117 n° 2 lit. a and section 117 n° 3 lit. a can be conducted by the criminal police at their own discretion.

#### **Section 121.**

(1) Prior to any search the affected person has to be requested, stating the relevant reasons, to admit the search or to voluntarily hand over the searched objects. This request can only be abandoned in the cases of imminent

danger and in the case of section 119 para. 2 n° 1. The application of force (section 93) is not permitted in the case of the search of a person according to section 119 para. 2 n° 3.

(2) The affected person has the right to be present in a search according to section 117 n° 2 and to be accompanied by a confidant(e) in this case and in the case of a search according to section 117 n° 2. For the confidant(e) section 160 para. 2 applies analogously. If the owner of a premise is not present, also an adult cohabitant can exercise his/her rights. If this is also not possible, two adult persons who are not affected have to be present. This can only be abandoned in cases of imminent danger. For a search of rooms only used to exercise the profession of one of the persons mentioned in section 157 para. 1 n° 2 to n° 4 ex officio a representative of the relevant legal representation organisation or the media owner or a representative named by him/her has to be called in.

(3) When a search is conducted, public attention, annoyances and disturbances have to be limited to the unavoidable amount. The owner's rights and the personality rights of all affected persons are to be respected as far as possible. A search of persons according to section 117 n° 3 lit. b always has to be conducted by a person of the same sex or by a doctor respecting the dignity of the examined person.

#### **Section 122.**

(1) The criminal police has to report as soon as possible to the office of public prosecution about every search according to section 120 para. 1 first sentence last half-sentence (section 100 para. 2 n° 2). The office of public prosecution afterwards has to apply for a judicial decision on the admissibility of the search (section 99 para. 3). If the search is not admitted the criminal police and the office of public prosecution have to restore the legal situation in accordance with the decision of the court using all means accessible to them.

(2) If during a search objects are found that lead to the conclusion that a criminal act different from the one regarding which the search was conducted has been committed, they have to be seized but a separate protocol has to be written about that and the incident has to be immediately reported to the office of public prosecution.

(3) In any case a confirmation of the search and its result and if applicable also the order of the office of public prosecution and the judicial decision have to be handed over or served to the affected person immediately or at the latest within 24 hours.

.../...

### **Part IV: Observation, undercover investigation and fictitious purchase**

#### **Definitions**

#### **Section 129.**

For the purpose of this law

1. "observation" is the secret surveillance of the conduct of a person,
2. "undercover investigation" is the use of officers of the criminal police or other persons on order of the criminal police, who do not disclose nor show their official position or their task,
3. "fictitious purchase" is the attempt or the feigned committing of a criminal act as far as this consist in the acquirement, purchase, possession, export, import or transport of objects or assets that have been alienated, originate from a crime or are dedicated to committing a crime or the possession of which is absolutely prohibited.

#### **Observation**

#### **Section 130.**

(1) An observation is admissible if it appears to be necessary in order to clarify a criminal act or to investigate the whereabouts of the accused.

(2) The use of technical means, that enable the establishment of an area in which the observed person is situated via the transmission of signals and the opening of vehicles and containers for the purpose of inserting such technical means is admitted as support for the observation if such observation otherwise would be futile or significantly hindered.

(3) As far as the observation

1. is supported by the use of technical means (para. 2),
2. is continued over a period of more than 48 hours or
3. is conducted or supposed to be conducted outside the area of Austria,

it is only admitted if there is the suspicion of an intentional criminal act punished with a prison sentence exceeding one year and if due to ascertained facts it can be assumed that the observed person has committed the criminal act or will establish contact with the accused or if with its help the whereabouts of the fugitive or absent accused can be established.

### **Undercover investigation**

#### **Section 131.**

(1) Undercover investigation is admitted if it appears to be necessary in order to clarify a criminal act.

(2) A systematic undercover investigation going on for a longer period of time is only admitted if clarifying an intentional criminal act punished with a prison sentence exceeding one year or the prevention of a criminal act planned within the framework of a criminal or terrorist association or a criminal organisation (sections 278 to 278b StGB) would otherwise be significantly hindered. As far as it is necessary for the clarification or prevention it is also admitted to produce documents in accordance with section 54a of the Austrian Police Act that fake the identity of an officer of the criminal police and to use such documents in the legal relations in order to fulfil the purpose of the investigation.

(3) The undercover agent has to be controlled by the criminal police and checked on a regular basis. His/her operations and the detailed circumstances of it as well as information and messages obtained by him have to be written down in a report or in an official annotation (section 95) as far as they can be significant for the investigation.

(4) Domiciles and other rooms protected by the right to sanctity of the home may only be entered by the undercover agent with permission of the owner. It is prohibited to obtain this permission by faking an access authorization.

### **Fictitious Purchase**

#### **Section 132.**

The realization of a fictitious purchase is admitted if the clarification of a crime (section 17 para. 1 StGB) or the seizure of objects or assets that originate from a crime or presumably are subject to forfeiture (section 20b StGB) or confiscation (section 26 StGB) would otherwise be significantly hindered. Under these prerequisites it is also admitted to participate in the realization of a fictitious purchase of third persons (section 12 3rd case StGB).

### **Joint Provisions**

#### **Section 133.**

(1) An observation according to section 130 para. 1 and an undercover investigation according to section 131 para. 1 can be realized by the criminal police at their own discretion. Observations according to section 130 para. 3 and undercover investigations according to section 131 para. 2 and the realization of a fictitious purchase according to section 132 have to be ordered by the office of public prosecution.

(2) An observation according to section 130 para. 3 and an undercover investigation according to section 131 para. 2 may only be ordered for the time necessary for fulfilling their purpose, at the longest for a period of one month, in the case of an undercover investigation for a maximum of three months. A new order is admitted as long as the prerequisites continue to exist and due to ascertained facts it can be assumed that continuing the observation or the undercover investigations will bring positive results. Section 99 para. 2 is not to be applied. Observations and undercover investigations have to be terminated as soon as the prerequisites do no longer exist, if their purpose is achieved or presumably can no longer be achieved or if the office of public prosecution orders the termination.

(3) Observation, undercover investigation and fictitious purchase have to be realized by the criminal police. The use of technical means for the optic or acoustic surveillance of persons in the framework of these investigation methods is only admitted upon fulfilling the prerequisites listed in section 136.

(4) After the termination of an observation according to section 130 para. 3 and the undercover investigation according to section 131 para. 2 and after finalizing the fictitious purchase the orders and judicial admissions according to para. 1 and 2 have to be served to the accused and affected persons if their identity is known or can be established without inappropriate efforts. Service can be postponed as long as it would endanger the purpose of the investigation in this or another proceeding.

## **Part V: Sequestration of letters, information on data of a transmission of communication and surveillance of communication and persons**

### **Definitions**

#### **Section 134.**

For the purpose of this federal law

1. “sequestration of letters” means opening and retaining telegrams, letters or other mail sent by or destined for the accused,
2. “information on data of a transmission of communication” means the disclosure of traffic data (section 92 para. 3 n° 4 of the Telecommunications Act [*Telekommunikationsgesetz – TKG*]), access data (section 92 para. 3 n° 4a TKG) and location data (section 92 para. 3 n° 6 TKG) of a communications service or an information society service (section 1 para. 1 n° 2 of the Notification Act [*Notifikationsgesetz*]),
3. “Surveillance of communication” means the investigation of the content of communication (section 92 para. 3 n° 7 TKG), that is exchanged or conveyed via a communications network (section 3 n° 11 TKG) or a service of the information society (section 1 para. 1 n° 2 Notification Act),
4. “optical and acoustic surveillance of persons” means the surveillance of the conduct of persons infringing their right to privacy and of the statements of persons that are not meant for the direct knowledge of third persons using technical means for transmitting and recording picture and sound without the knowledge of the affected persons,
4. “result” (of the sequestration, information or surveillance mentioned in n° 1 to 4) means the content of letters (n° 1), the data of a communication surveillance or the content of transmitted communications (n° 2 and 3) and the picture and sound recordings of a surveillance (n° 4).

### **Sequestration of letters, information on the data for a communications transmission and surveillance of communications**

#### **Section 135**

(1) The sequestration of letters is admitted if it is necessary for clarifying an intentional criminal act punished with a prison sentence exceeding one year and if the accused is imprisoned for such an act or if his production or arrest has been ordered regarding that act.

(2) Disclosure of information on the data for a communication transmission is admitted

1. if and as long as there is the urgent suspicion that a person affected by the information has abducted another person or otherwise taken this person into his/her power and if the information is limited to data of such communication which presumably has been transmitted, received or sent by the accused at the time of the deprivation of liberty,
  2. if it can be expected that it contributes to clarifying an intentional criminal act punished with a prison sentence exceeding six months and if the holder of the technical device that was or will be origin or destination of the transmission of communications explicitly agrees, or
  3. if it can be expected that it contributes to clarifying an intentional criminal act that is punished with a prison sentence exceeding one year and if due to ascertained facts it can be assumed that in this way data of the accused can be established.
- (3) Surveillance of communications is admitted,
1. in the cases of para. 2 n° 1,
  2. in the cases of para. 2 n° 2 if the holder of the technical device that was or will be origin or destination of the transmission of communications agrees to the surveillance,
  3. if it appears to be necessary to clarify an intentional criminal act punished with a prison sentence exceeding one year or if otherwise clarifying or preventing criminal acts planned or committed in connection with a criminal or terrorist association or a criminal organisation (sections 278 to 278b StGB) would be significantly hindered and  
the holder of the technical device that was or will be the origin or destination of the transmission of communications is urgently suspected of committing the intentional criminal act punished with a prison sentence exceeding one year or a criminal act according to sections 278 to 278b StGB, or if due to ascertained facts it can be assumed that a person suspected of committing the act (lit. a) will use the technical device or will establish a connection with it;
  4. if due to ascertained facts it can be expected that the whereabouts of a fugitive or absent accused who is urgently suspected of having committed an intentional criminal act punished with a prison sentence exceeding one year can be established through it.

**ARHG (Law on Extradition and Mutual Assistance)**

**TITLE I: General Provisions**

.../...

**Reciprocity**

**§ 3.** (1) A foreign request may only be complied if it is ensured that the requesting State would also comply with a similar request by Austria.

(2) A request under this federal law may not be filed by an Austrian authority if it were not possible to comply with a similar request by another State, unless a request appears to be needed urgently for specific reasons. In this case, the requested State shall be notified of the absence of reciprocity.

(3) In the event of doubts concerning compliance with reciprocity, the opinion of the Federal Minister of Justice shall be obtained.

(4) Another State may be assured of reciprocity in connection with a request made under this federal law, provided that there are no intergovernmental agreement and that it would be admissible under this federal law to comply with a similar request of this State.

**Conditions**

**§ 4.** There shall be compliance with the conditions that another State imposes on the occasion of granting an extradition, transit or surrender, when providing judicial assistance, or in connection with taking over a case for criminal prosecution, surveillance, or execution, and which were not rejected.

.../...

**Application of the Code of Criminal Procedure**

**§ 9.** (1) Unless the provisions of this federal law stipulate otherwise, the 1975 Code of Criminal Procedure, Federal Law Gazette No. 631/1975, shall be applied in analogy.

(2) § 64, § 71 to § 73 and § 381 to § 392 of the Code of Criminal Procedure shall not be applied to proceedings for the extradition of persons; § 51 to § 53 and § 59 (2) of the Code of Criminal Procedure, however, shall only apply with the proviso that the date of the examination of the person concerned on the application for extradition (§ 31 (1)) shall replace the filing of the bill of indictment.

(3) The public prosecutor may refrain from prosecuting a punishable act and discontinue the investigating procedure accordingly, provided that the Austrian criminal jurisdiction is only based on § 65 (1) item 2 of the Criminal Law Code and that public interests do not oppose such refraining from prosecution, in particular, if punishment is not required in order to deter others from committing punishable acts.

(4) If surveillance of a person convicted by a foreign court is to be taken over, or if the decision of a foreign court is to be enforced, the public prosecutor may refrain from prosecuting the criminal act underlying the foreign conviction and discontinue the investigative proceedings accordingly, if it can be assumed that the Austrian court would not impose a considerably more severe punishment or preventive measure than the one imposed by the foreign court.

**TITLE II: Extradition from Austria**

**CHAPTER ONE: Admissibility of Extradition**

**General Principle**

**§ 10.** The extradition of persons to another State for the purpose of prosecution for acts subject to punishment by court or for the execution of a custodial sentence or a preventive measure imposed for such an act shall be admissible at the request of another State according to the provisions of this federal law.

### **Punishable Acts Qualifying for Extradition**

§ 11. (1) Extradition shall be admissible for the prosecution of intentionally committed acts that are punishable under the law of the requesting State by a custodial sentence of more than one year or by a preventive measure of the same duration and that are subject to a custodial sentence of more than one year under Austrian law. The penal sanctions, as amended by § 5 item 4 of the 1988 Juvenile Court Act shall not be used as a basis for deciding whether a punishable act shall give rise to an extradition. It is irrelevant whether an application, as required for prosecution under Austrian law, has been made or such an authorization has been given.

(2) An extradition for execution shall be admissible in cases where the custodial sentence or the preventive measure has been imposed for one or several of the punishable acts listed in paragraph (1) and when a remaining period of at least four months still needs to be executed. Several custodial sentences or the remaining parts thereof shall be aggregated.

(3) If an extradition is admissible under paragraphs (1) or (2), a person may also be extradited for the prosecution of other punishable acts or for the execution of other custodial sentences or preventive measures, in cases where extradition would otherwise not be admissible on account of the term of the stipulated sanction (paragraph (1)) or of the duration of the punishment or measure (paragraph (2)).

### **Prohibition to Extradite Austrian Citizens**

§ 12. (Constitutional provision) (1) The extradition of Austrian citizens shall not be admissible. (2) Paragraph (1) shall not prevent the return of an Austrian citizen who a foreign authority has surrendered to the Austrian authorities only temporarily for the purpose of performing specific procedural steps or in connection with providing of judicial assistance.

### **Primacy of Extradition**

§ 13. If extradition proceedings are pending against a foreign citizen, or if there are sufficient grounds to institute such proceedings, it shall not be admissible to remove him/ her from Austria on the basis of other legal provisions.

### **Punishable Acts of a Political Nature**

§ 14. Extradition shall not be admissible:

1. for political offences,
2. for other punishable acts that are based on political motives or aims, unless the criminal nature of the act outweighs its political nature, when taking into consideration all the circumstances of a specific case, especially the way in which the offence has been committed, the means applied or threatened, or the severity of the actual or intended consequences.

### **Military and Fiscal Punishable Acts**

§ 15. Extradition shall be not be admissible for punishable acts which, according to Austrian law, are exclusively of a military nature, or constitute a violation of stipulations relating to taxes, monopolies or customs duties, or of foreign exchange regulations, or of stipulations relating to the control of or foreign trade in goods.

### **Austrian Jurisdiction**

§ 16. (1) An extradition for punishable acts that are subject to Austrian jurisdiction shall be prohibited.

(2) However, paragraph (1) does not oppose extradition if

1. jurisdiction is only exercised on behalf of another country, or
2. precedence shall be given to conducting the criminal proceedings in the requesting State, taking special circumstances into account, particularly reasons of ascertaining the truth, of determining or executing a punishment.

(3) In the cases defined in paragraph (2), extradition shall also not be admissible if the person to be extradited has already been convicted or acquitted with final and enforceable effect in Austria, or has been exempted from prosecution for reasons other than those specified in § 9 (3). In cases pursuant to paragraph (2) item 2 extradition shall also be inadmissible if there is reason for concern that, on account of the conviction in the other State, the person to be extradited would be in a significantly worse position overall than would be the case under Austrian law.

#### **Jurisdiction of a Third Country**

§ 17. An extradition shall be inadmissible if the person to be extradited for a punishable act

1. has been acquitted with final and enforceable effect by a court of the State in which the offence was committed, or has otherwise been exempted from prosecution, or
2. has been convicted with final and enforceable effect by a court in a third country, and the punishment has been fully served or waived in whole or in part for the portion of the sentence remaining to be enforced, or if the enforceability of the punishment comes under the statute of limitation pursuant to the law of this third country.

#### **Limitation**

§ 18. An extradition shall be inadmissible if prosecution or execution comes under the statute of limitations in accordance with the laws of the requesting State or under Austrian law.

#### **Compliance with the Principles of the Rule of Law; Asylum**

§ 19. An extradition shall be inadmissible if there is reason to suspect that

1. the criminal proceedings in the requesting State will not comply or did not comply with the principles of Articles 3 and 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Federal Law Gazette No. 210/1958,
2. the punishment or preventive measure imposed by or to be expected in the requesting State would be enforced in a manner that is not consistent with the requirements of Article 3 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Federal Law Gazette No. 210/1958, or the person to be extradited would be subject to persecution in the requesting State because of his/her origin, race, religion, affiliation to a specific ethnic or social group, nationality, or political opinions, or would have to expect other serious prejudices for any of these reasons (extradition asylum).

#### **Inadmissible Punishments or Preventive Measures**

§ 20. (1) Extradition for prosecution of a punishable act subject to capital punishment under the laws of the requesting State shall only be admissible if it is ensured that the death penalty will not be imposed.

(2) Extradition for execution of the death penalty shall be inadmissible.

(3) The provisions of paragraphs (1) and (2) shall also apply in analogy to punishments or preventive measures that do not comply with the requirements of Article 3 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Federal Law Gazette No. 210/1958.

#### **Prosecution of Persons without Criminal Responsibility**

§ 21. It shall be inadmissible to extradite persons who were without criminal responsibility under Austrian law or the law of the requesting State at the time of the punishable act.

#### **Hardship Cases**

§ 22. It shall be inadmissible to extradite persons who would be exposed to obviously disproportionately severe conditions when considering the severity of the punishable act with which they are charged, their young age (§1 item 2 of the 1988 Juvenile Court Act), the long period of their residence in Austria, or other serious reasons based on their personal circumstances.

.../...

### **Processing of Received Requests**

**§ 30.** The Federal Ministry of Justice shall forward extradition requests for further processing directly to the competent public prosecutor's office, informing the senior public prosecutor's office at the same time. The Federal Minister of Justice shall reject a request directly if circumstances prevail that oppose an extradition for any of the reasons listed in § 2 and § 3 (1) or if the request is unsuited for being processed lawfully.

### **Proceedings on the Admissibility of an Extradition**

**§ 31.** (1) The court shall examine the person concerned in connection with the extradition request. § 29 (3) shall apply in analogy. The court shall decide on the admissibility of an extradition by way of a court decision in accordance with § 33.

(2) The decision shall be taken on the basis of a public oral hearing if the person concerned or the public prosecutor so move, or if the court deems it necessary in order to examine the admissibility of the extradition. If the person concerned is kept detained pending extradition, the hearing on the admissibility of the extradition shall take place in the course of a hearing on the detention in accordance with the provisions of paragraph (3). Irrespective of an application to hold a hearing, the court may always state that an extradition is inadmissible without holding a hearing. If the court decides without a hearing, the person concerned and his/her defense counsel, as well as the public prosecutor must have been given an opportunity in any event to comment on the request for extradition.

(3) The person concerned must be represented at the hearing by a defense counsel (§ 61 (1) of the Code of Criminal Procedure). If the person concerned is being detained, steps shall be taken for his/her production in court, unless he/she expressly waived being present in court through his/her defense counsel. § 172 of the Code of Criminal Procedure shall be applied in analogy.

(4) Except for the cases listed in § 229 of the Code of Criminal Procedure, the public may be excluded from the hearing, if this might affect bilateral relations. In the hearing the single judge shall first present a summary of the content of the documents received by the court and the course of the proceedings up to the hearing. The public prosecutor shall then be given leave to speak. Next, the person concerned and his/her defense counsel shall be given an opportunity to comment on the request for extradition and the statements by the public prosecutor. In any event, the person concerned and his/her defense counsel shall have the right to make the final statement.

(5) The single judge shall proclaim the decision on the admissibility of the extradition and explain the reasons for the decision. The decision shall be issued in writing and shall indicate those facts, in any event, that were decisive for stating that the extradition is admissible or inadmissible.

(6) If, in the event of an oral proclamation of the decision, the person concerned or the public prosecutor files a complaint within three days, the complainant may state further details of the complaint within fourteen days after having received the written copy. The complaint has suspensive effect. The provisions on the proceedings before the appellate court (§ 89 of the Code of Criminal Procedure) shall apply with the proviso that the higher regional court shall decide on the complaint in a public oral hearing, applying § 294 (5) of the Code of Criminal Procedure in analogy, unless the complaint must be rejected as inadmissible pursuant to § 89 (2) first sentence of the Code of Criminal Procedure. The higher regional court shall submit its decision to the Federal Ministry of Justice, attaching the case file.

(7) If no complaint is filed, the court shall submit the case file directly to the Federal Ministry of Justice.

### **Simplified Extradition Procedure**

**§ 32.** (1) On the basis of a foreign request for extradition or for imposing detention pending extradition, the person concerned may state his/her consent to the extradition and agree to being transferred without conducting the formal extradition proceedings. However, if several requests have been submitted, the consent statement is

only effective if it covers all requests. However, if the person concerned is detained pending extradition, he/she may state his/her consent at the earliest at the hearing on the detention, which must be held pursuant to § 175 (2) item 1 of the Code of Criminal Procedure. In any event, the consent will only become legally valid if it is put on record by the court.

(2) The court shall inform the person concerned that, in the event of an extradition pursuant to paragraph (1), he/she shall not be entitled to the protection afforded by § 23 (1) and (2) or by the corresponding provisions of intergovernmental agreements and that he/she may not revoke his/her consent.

(3) The simplified extradition of a juvenile shall only be admissible if his/her legal representative also consents or if he/she is represented by a defense counsel.

(4) If a person concerned has consented to the simplified extradition procedure, the court shall submit the case file directly to the Federal Ministry of Justice.

.../...

## **TITLE IV: Judicial Assistance to Foreign Countries**

### **CHAPTER ONE: Requirements**

#### **General Principle**

**§ 50.** (1) In accordance with the provisions of this federal law, judicial assistance may be granted in criminal matters upon a request by a foreign authority, including proceedings to order preventive measures and to issue a property-law order, as well as in matters of extinction and the register of criminal records, in proceedings to obtain compensation for confinement and conviction by a criminal court, in clemency petition matters and in matters concerning the execution of sentences and measures. With the proviso of § 59a, the transfer of data to a foreign authority shall be admissible without such a request.

(2) An authority within the meaning of paragraph (1) shall be a court, a public prosecutor's office, or an agency acting in matters concerning the execution of sentences or measures.

(3) Judicial assistance within the meaning of paragraph (1) shall be any support that is provided in connection with foreign proceedings in a criminal-law matter. It also includes consenting to activities as part of cross-border observations on the basis of intergovernmental agreements.

#### **Inadmissible Judicial Assistance**

**§ 51.** (1) Providing judicial assistance shall not be admissible to the extent that

1. the act underlying the request is either not subject to punishment by a court under Austrian law or does not qualify for extradition pursuant to § 14 und § 15,
2. extradition would be inadmissible pursuant to § 19 items 1 and 2 for the proceedings underlying the request, or
3. either the practical requirements to perform specific investigative measures, as defined in Title 8 of the Code of Criminal Procedure, do not prevail, or providing judicial assistance would result in a violation of the obligation of confidentiality, to be also observed vis-à-vis criminal courts under Austrian law (§ 76 (2) of the Code of Criminal Procedure).

(2) The absence of criminal liability under Austrian law shall not oppose the service of documents if the recipient is prepared to accept them.

.../...

### **CHAPTER THREE: Execution of Foreign Criminal-Court Decisions**

#### **Prerequisites**

**§ 64.** (1) The execution or further execution of a decision by a foreign court imposing a fine or custodial sentence, a preventive measure or property-law order with final and enforceable effect shall be admissible upon a request by another State if:

1. the decision of the foreign court was taken in proceedings complying with the principles set forth in Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Federal Law Gazette No. 210/1958,
  2. the decision was taken for an act that is sanctioned by a court punishment under Austrian law,
  3. the decision was not taken for one of the punishable acts listed in § 14 and § 15,
  4. under Austrian law no statute of limitation applies to the execution,
  5. the person concerned by the decision of the foreign court is not prosecuted for an act in Austria, has not been convicted or acquitted with final and enforceable effect or otherwise been exempted from prosecution.
- (2) The execution of a decision by a foreign court imposing a custodial sentence or preventive measure shall only be admissible if the convicted person is an Austrian citizen, has his/her domicile or place of residence in Austria and has agreed to the execution in Austria.
- (3) The execution of preventive measures shall only be admissible if Austrian law provides for a similar measure.
- (4) The execution of a decision by a foreign court issuing property-law orders shall only be admissible if the decision complies with the prerequisites for fines, the skimming off of an enrichment, forfeiture or seizure under Austrian law and a comparable domestic order has not yet been issued in Austria.
- (5) Moreover, the execution of a decision by a foreign court imposing a fine or the skimming off of an enrichment shall only be admissible if its collection in Austria may be expected and the person concerned has been heard, to the extent that he/she can be contacted.
- (6) Moreover, the execution of a decision a foreign court imposing forfeiture or seizure with final and enforceable effect shall only be admissible if the objects or property items covered by the decision are located in Austria and the person concerned has been heard, to the extent that he/she can be contacted.
- (7) Fines, skimmed off amounts of money, forfeited property items and seized objects shall accrue to the Federal State.

#### **Austrian Decisions on Execution**

**§ 65.** (1) If the execution of a foreign court decision in criminal matters is taken over, the punishment, the preventive measure or the property-law order to be executed shall be determined according to Austrian law, taking account of the measure imposed in the decision. A decision by a foreign court ordering forfeiture may also be executed as an act of forfeiture in Austria, if an enrichment would have to be skimmed off under Austrian law.

- (2) The person concerned by the decision may not be put into a more adverse position because of the fact that the execution is taken over than he/she would be in if the execution took place in the other State.
- (3) § 38 and § 66 of the Criminal Law Code shall apply in analogy.

#### **Processing of Incoming Requests**

**§ 66.** The Federal Ministry of Justice shall forward requests for the execution of foreign criminal-court decisions to the competent regional court (§ 67 (1)). The Federal Minister of Justice shall immediately refuse a request if circumstances have emerged already at the time when the request is received that render it inadmissible to take over the execution for one of the reasons in listed in § 2 and § 3 (1) or if the request is not suited for lawful processing. At any stage of the procedure the Federal Minister of Justice may demand

additional documents from the State requesting that an execution be taken over, either his/her own initiative or upon application by the first-instance court.

### **Competences and Procedures**

§ 67. (1) The regional court in whose district the person concerned has his/her domicile or place of residence shall be responsible for requests to execute or adapt the punishment, preventive measure or skimming off of an enrichment. If these provisions do not result in any specific competences of a specific regional court, the Regional Court for Criminal Matters in Vienna shall have jurisdiction. The regional court in whose district the property item or object is located shall be responsible for requests on executing a decision on forfeiture or seizure (§ 31 (5) of the Code of Criminal Procedure).

(2) The Federal Minister of Justice shall inform the requesting State of the decision concerning the request for taking over the execution, as well as of the actual execution, by way of the established channels of communication.

(3) After a punishment or preventive measure has been taken over for execution, criminal proceedings may no longer be lodged for the act underlying the court decision.

(4) The provisions under Austrian law shall apply to the execution, release on probation, as well as to clemency acts.

(5) Execution shall be discontinued in any event if the enforceability of the punishment or preventive measure expires under the law of the requesting State.

## EU-JZG (Law on Judicial Cooperation in Criminal Matters with EU Member States)

.../...

### Part Two: Execution of Decisions on Seizure by Member States

#### Prerequisites

**§ 45.** (1) A decision on the freezing of evidence may be taken or executed for criminal offences that carry a court punishment pursuant to the law of the deciding State and, with the proviso of the provision of paragraph (3), pursuant to the law of the executing State.

(2) A decision on the freezing of property that might subsequently become the subject to a collection, skimming off of the enrichment or forfeiture, may be issued or executed if, in accordance with paragraph (3), the law of the deciding State and of the executing State allow a freezing.

(3) For a decision pursuant to paragraphs (1) or (2) double criminality need not be verified if the offence underlying the freezing order was assigned to one of the categories of offences listed in Annex I and carries a maximum custodial sentence of at least three years according to the law of the issuing State..

(4) The freezing order will only be executed if it is accompanied by a certificate in the form shown in Annex II. If the certificate is incomplete, or if it obviously does not correspond to the freezing order, the issuing judicial authority may be set a time limit for completing or correcting the information, if the available documents are not sufficient for a decision on the execution of the freezing order.

#### Competences and Procedure

**§ 46.** (1) The regional court with jurisdiction for the location of the property or evidence shall decide on the execution of a freezing order by another Member State. The issuing judicial authority shall be informed of the filing of the complaint, as well as of the outcome of the procedure on the complaint.

(2) A request for executing a freezing order which requires a procedure deviating from Austrian criminal procedural law, shall be satisfied, if this can be reconciled with the criminal proceedings and its principles pursuant to Chapter 1 of the Code of Criminal Procedure.

(3) The court shall decide as expeditiously as possible on the freezing order, if possible within 24 hours after receiving the request, and shall inform the issuing State of its decision.

#### Refusal to Execute

**§ 47.** (1) It is inadmissible for an Austrian judicial authority to execute a freezing order if

1. the prerequisites according to § 45 do not prevail,
2. there are privileges and immunities under Austrian law that make it impossible to execute a freezing order, or
3. the certificate (§ 45 (4)) indicates that by executing a decision on collection or forfeiture the principle listed in § 7 (1) were to be violated.

(2) In criminal matters relating to charges, taxes, customs and foreign exchange transactions the execution of a freezing order cannot be refused by giving as a reason that Austrian law does not contain provisions on charges, taxes, customs or foreign-exchange transactions of the same type as under the law of the issuing State.

#### Postponing an Execution

**§ 48.** (1) The execution of a freezing order shall be postponed if the property or the evidence was already confiscated in the course of proceedings pending in Austria or seized.

(2) If the confiscation or seizure in domestic proceedings is lifted, a decision shall be taken immediately on the execution of the freezing order.

(3) The execution of a freezing order may be postponed for as long as it would jeopardize the purpose of the pending investigations.

#### **Duration of Confiscation or Freezing**

§ 49. If no request for delivery of the evidence or execution of a forfeiture or collection decision is enclosed with the freezing order, by annexing the decision to be executed, the confiscation or freezing shall be maintained until a decision is reached concerning the request for judicial assistance of the issuing State relating to the evidence or property in question, provided that the prerequisites for confiscation or freezing under the present provision continue to apply. Moreover, the procedure shall comply with the third sentence of § 58 of the ARHG.

#### **Obligation to Inform**

§ 50. If the execution of a freezing order proves to be inadmissible, to be actually impossible or requires postponing, the court shall forward this information immediately to the issuing authority. The same shall apply to appeals against the execution and the performed execution of the freezing order.

#### **Exchanges between Authorities and Translations**

§ 51. (1) § 14 shall apply in analogy to the exchanges between authorities on the execution of a freezing order.

(2) The certificate according to Annex III relating to freezing orders by Austrian courts shall be translated into the official language of the Member State in which the freezing order is to be executed; unless that State has issued a statement that it will accept a translation into German or another language.

### **Part Three: Execution of Orders Relating to Property Rights**

#### **Subdivision One: Execution of Decisions Taken by Other Member States**

##### **Prerequisites**

§ 52. (1) An order relating to property rights, issued with final and enforceable effect by a court of another Member State, shall be executed in accordance with the provisions of the present Part Three.

(2) An order relating to property rights is a decision taken after conducting criminal-law proceedings requiring the withdrawal of sums of money or objects (forfeiture, dispossession; § 20b and § 26 of the Criminal Law Code) or of a sum of money taking their place (absorption of the enrichment; § 20 of the Criminal Law Code). Financial penalties, victim compensations and costs of proceedings shall not constitute orders relating to property rights.

##### **Inadmissible Executions**

§ 52a. (1) It shall be inadmissible for an Austrian court to execute orders relating to property rights by another Member State,

1. if the offence underlying the order relating to property rights or – in the case of money laundering pursuant to § 165 of the Criminal Law Code the preceding offence –

a) was committed in Austria or on board of an Austria vessel or aircraft, or

b) outside the national territory of the deciding State if – under Austrian law – offences of this kind committed outside the national territory would not fall within the scope of Austrian criminal law;

2. if a final and enforceable order relating to property rights was already imposed upon the person concerned for the offence underlying the order relating to property rights in Austria, or a final order relating to property rights was issued by another State and has already been executed;

3. if the offence underlying the order relating to property rights is not punishable by a court according to Austrian law, unless the offence can be assigned to one of the categories of offences listed in Annex 1, Part A; the classification made by the deciding State is binding with the proviso of § 52c (2) item 3;

4. if enforceability has lapsed according to Austrian law of the order relating to property rights, which is based on an offence that falls within the scope of Austrian criminal laws;
5. if the person concerned has been granted amnesty or pardon in Austria or the deciding State;
6. if execution were to violate provisions on immunity;
7. if the rights of innocent third parties oppose execution;
8. if the hearing leading to the order relating to property rights was conducted in the absence of the person concerned and that person was not represented by a legal counsel, unless he/she was informed of the hearing, either in person or through a representative authorized according to the law of the deciding State, in keeping with the statutory provisions of that State and stated that he/she will not challenge the order relating to property rights;
9. if the order relating to property rights comprises an expanded collection which it would not be possible to impose according to § 20 (2) or (3) of § 20b of the Criminal Law Code;
10. if there are objective indications that the decision was taken in violation of fundamental rights or essential legal principles in accordance with Article 6 of Treaty on European Union, especially if the order relating to property rights was issued for the purpose of punishing the person concerned for reasons of his/her sex, race, religion, ethnic origin, nationality, language, political conviction or sexual orientation and the person concerned did not have any possibility to claim this circumstance before the European Court of Human Rights or before the European Court of Justice.

(2) In matters relating to levies, taxes, customs duties and currency issues, execution of an order relating to property rights must not be refused on the ground that Austrian law does not require payment of equivalent levies or taxes, or does not contain any provisions on levies, taxes, customs duties and currency issues that are equivalent to those under the law of the deciding State.

#### **Competences**

**§ 52b.** (1) The regional courts shall have subject-matter jurisdiction for decisions on the execution of orders relating to property rights.

(2) The court venue shall be guided by the place in which the sum of money or the object covered by the order relating to property rights is located, or where the person concerned makes dispositions concerning his/her property, in which connection the decision may be enforced. If these places cannot be identified, that place shall be decisive where the person concerned has his/her domicile or residence; in the case of an association (§ 1 (2) and (3) of the VbVG) it shall also be the place where it has its office, its operation or its branch office. If the competences of a specific court cannot be ascertained on the basis of the present provisions, the Regional Court for Criminal Matters in Vienna shall have jurisdiction.

(3) If the court that was seized with the execution does not have jurisdiction, it shall transfer the matter to the competent court.

#### **Procedure**

**§ 52c.** (1) Execution requires that the decision to be executed and the certificate (Annex V) to be signed by the competent authority and – unless the deciding State submitted a statement to the effect that, as an executing State, it will also accept certificates in the German language (§ 52k (2)) – their translations into the German language are forwarded to the Austrian court.

(2) If

1. the certificate was not forwarded, is incomplete in major parts or is in obvious contradiction to the order relating to property rights,

2. there are indications that one of the reasons listed in § 52a (1) items 1, 2, and 7 to 10 applies, rendering execution inadmissible,
  3. the legal classification as an offence according to Annex I, Part A, is obviously erroneous, or if the person concerned has raised justified objections against it, or
  4. the person concerned documents that the sum of money or the object covered by the order relating to property rights has already been collected, that the order relating to property rights which refers to a sum of money has already been partly executed, or that he/she already paid a sum of money on the basis of such a decision, the authority of the deciding State shall be requested to forward the certificate subsequently, to complete it or to supplement the information within a time period to be fixed, pointing out that execution will be refused altogether or in part if the time limit expires unsuccessfully.
- (3) § 14 (1) to (5) shall apply to the exchanges between authorities.
- (4) If the person concerned by the decision can be summoned in Austria, he/she shall be heard concerning the prerequisites for execution (§ 52, § 52a), concerning the issue of an already performed collection of the sum of money or the object covered by the order relating to property rights, as well as concerning the amount of the sum to be executed.

### **Decision**

- § 52d.** (1) A decision shall be taken on execution. The decision shall indicate the name of the authority, whose decision is executed, its file number, a brief presentation of the facts, including the time and place of the offence and the measures contained in the order, the name of the punishable offence, as well as the legal provisions applied by the deciding State.
- (2) If execution is accepted for an order relating to property rights that is issued for a sum of money, the sum to be executed in Austria shall be fixed as that amount of money which is indicated in the decision that is to be executed. If the amount is not euros, it shall be converted at the exchange rate applicable on the day on which the decision on execution is taken. Previously made payments and contributed amounts shall be taken into account.
- (3) The public prosecutor and the person concerned by the decision shall have the right to file a complaint against the decision to the higher regional court within 14 days. A complaint that is filed in time shall have suspensive effect.
- (4) The procedure described in § 408 of the Code of Criminal Procedure shall be applied, once the decision has become final and enforceable.
- (5) If execution is refused for one of the reasons given in § 52a (1), the public prosecutor shall report this to the Federal Ministry of Justice, enclosing a copy of the decision.

### **Postponing Execution**

- § 52e.** (1) The execution of an order relating to property rights shall be postponed
1. for as long as no final and enforceable decision has been taken on an admissible complaint (§ 52d (3));
  2. if the deciding State also seized other Member States with the execution of the order relating to property rights and the total executed amount might exceed the sum of money fixed in the order relating to property rights;
  3. for as long as the sum of money or the object is the basis of proceedings in Austria that may result in an order relating to property rights;
  4. for as long as the purpose of ongoing investigations may be jeopardized;

5. for the time considered necessary by the court for obtaining a translation, at its expense, of the order relating to property rights;

6. until the additional information requested from the competent authority of the deciding State has been received.

(2) If there is concern that the sum of money or the object will no longer be available for the purposes of executing the order relating to property rights, once the reason for as deferral no longer applies, the court shall take all admissible measures, including issuing a temporary injunction according to § 144a of the Code of Criminal Procedure, during the period of the deferral.

#### **Orders Relating to Property Rights Issued by Several Member States**

**§ 52f.** If two or several Member States forward orders relating to property rights

1. concerning the same object, or
2. a sum of money attributable to the same person concerned, without that person having the means in Austria that suffice for an execution of all decisions,

a decision shall be taken as to which order relating to property rights or which orders relating to property rights shall be executed, giving due consideration to all circumstances, especially whether the sum of money or the object has already been frozen according to Part II of Chapter III of the present federal law, to the seriousness of the punishable offences underlying the orders relating to property rights, the place of the offence, the dates at which the orders relating to property rights were issued and the time sequence of their communication.

#### **Proceeds from Execution**

**§ 52g.** (1) Sums of money obtained by executing the order relating to property rights, which are not in excess of EUR 10,000 or the equivalent of that amount, shall accrue to the Federal State. If the sum of money obtained by executing the order relating to property rights is in excess of EUR 10,000, 50% of the amount shall be transferred to the deciding State.

(2) Objects that have been obtained by executing an order relating to property rights shall be sold in keeping with the provisions in § 377 of the Code of Criminal Procedure. Paragraph (1) shall apply to the arrangements concerning the proceeds. If such a procedure cannot be followed, and if the deciding State does not consent to the transfer of the objects, they shall accrue to the Federal State.

(3) Paragraphs (1) and (2) shall only be applied if no other agreements have been reached with the deciding State.

(4) Objects that are part of Austria's cultural heritage shall accrue to the Federal State in any event.

#### **Discontinuing Execution**

**§ 52h.** If the competent authority of the deciding State communicates that the order relating to property rights or its enforceability have been revoked, or that execution is no longer requested for some other reason, execution shall be discontinued.

#### **Informing the Deciding State**

**§ 52i.** The court shall inform the competent authority of the deciding State without delay in the event that

1. it transfers the case to the competent court (§ 52b (3)),
2. the sum to be executed has been fixed at an amount which is lower than the amount for which the order relating to property rights was issued (§ 52d (2)),
3. execution has been postponed, indicating the reasons and, if possible, the presumed duration of the deferral,

4. the decision has been enforced,
5. execution is refused in full or in part, indicating the reasons,
6. the order relating to property rights cannot be executed because the sum of money or the object have disappeared, were destroyed, cannot be collected in Austria or cannot be found at the location indicated in the certificate, because the place at which the sum of money or the object is to be found has not been identified with sufficient precision, or because another order relating to property rights has already been executed concerning the sum of money or the object (§ 52f), always indicating the reasons.

#### **Costs**

**§ 52j.** The costs incurred by executing a foreign order relating to property rights shall be borne by the Federal State, irrespective of whether they can be collected from the person concerned. If considerable or extraordinary costs have been incurred on account of the collection, a sharing of the costs shall be proposed to the authority of the deciding State, attaching a detailed break-down of the costs.

#### **Subdivision Two: Obtaining Execution in Another Member State**

##### **Seizing Another Member State**

**§ 52k.** (1) Whenever there is reason to seize another Member State with the execution of an order relating to property rights, the court that has taken the first-instance decision must first allow the public prosecutor time to comment and to hear the person concerned, if he/she can be summoned in Austria.

(2) The court shall forward to the competent authority of the executing State

1. the decision to be executed, complete with a translation, if such a translation was already made for the foreign person concerned in the proceedings in Austria, as well as
2. a completed and signed certificate (**Annex 5**) and, if the executing State did not indicate that it also accepts certificates in the German language, a translation of the certificate into one of the official languages of the executing State or into another language accepted by it.

The Federal Minister of Justice shall proclaim by way of ordinance which Member States accept which official languages.

(3) § 14 (1) to (5) shall apply in analogy to the exchanges between the authorities. If the decision and the certificate were not communicated by mail, the competent authority of the executing State shall subsequently be sent by mail, upon its request, a specimen or a certified copy of the decision, as well as the original of the certificate.

##### **Forwarding an Order Relating to Property Rights to Several Executing States**

**§ 52l.** (1) Subject to paragraphs (2) and (3) an order relating to property rights must always be sent to only one executing State in every case.

(2) An order relating to property rights concerning specific objects may be sent to several executing States at the same time if

1. there is reason to assume that objects covered by the order relating to property rights are located in several executing States,
2. the execution of the order relating to property rights requires measures in several executing States, or
3. there is reason to assume that an object covered by the order relating to property rights is located in one or two or several known executing States.

(3) An order relating to property rights issued for an amount of money may be communicated to several executing States at the same time, if this is required for its collection, especially if the amount of money was not secured pursuant to the provisions of Part Two of Chapter III of the present federal law, or if the execution by only one executing State will probably not be sufficient to collect the entire amount of money for which the order relating to property rights was issued.

#### **Execution in Austria**

**§ 52m.** The execution proceedings in Austria may be continued, even though the order relating to property rights was communicated to one or several executing States. However, the total amount obtained by way of executing the decision on the collection of amount of money must not exceed the amount indicated in the decision.

#### **Informing the Executing State**

**§ 52n.** The court that took the first-instance decision shall inform the competent authority of the executing State without delay if:

1. in the event of a risk of execution in excess of the order relating to property rights issued for an amount of money, that risk has ceased,
2. the decision was executed in full or in part in Austria or in another executing State, possibly indicating the amount which has not yet been collected by execution,
3. the person concerned already paid an amount of money, as a result of the order relating to property rights,
4. the order relating to property rights or its enforceability was subsequently lifted or modified, or if the execution is no longer requested for other reasons.”

### **Part Four: Execution of Pecuniary Sanctions**

#### **Subdivision One: Execution of Decisions Taken by Other Member States**

##### **Prerequisites**

**§ 53.** (1) A final and enforceable decision taken by a court of another Member State issued for a pecuniary sanction (paragraph (3)), due to an offence punishable by court pursuant to the law of that State, shall be executed in accordance with the provisions of the present Part Four.

(2) The following shall be considered to decisions pursuant to paragraph (1):

1. the decision of another judicial authority, especially of a public prosecutor, if the person concerned was given the opportunity of bringing the matter before a court that also has criminal-law competences, as well as
2. the decision of a court that also has criminal-law competences which was seized with an appeal against a decision that was taken by another than a judicial authority for a punishable act, administrative trespass or breach of an administrative regulation in keeping with the law of the deciding State.

(3) A pecuniary sanction shall be

1. financial penalties,
2. an obligation imposed by the same decision to pay compensation to the victim, if the victim did not have the possibility to submit civil-law claims in the course of the proceedings and the court took action by exercising its criminal-law competences,
3. the obligation to refund the costs of the proceedings leading to the decision, or

4. an obligation imposed in the same decision to pay an amount of money into a public account or to an organization supporting victims.

Orders relating to property rights shall not be considered to be pecuniary sanctions if they were to be classified as skimming off an enrichment, forfeiture or confiscation under Austrian law, as well as court decisions on private-law claims.

### **Inadmissible Executions**

**§ 53a.** It shall be inadmissible for an Austrian court to execute the decision of another Member State which imposes a pecuniary sanction,

1. if the pecuniary sanction is less than the amount of EUR 70 or its equivalent,
2. if the offence underlying the decision
  - a) was committed in Austria or on board of an Austrian vessel or aircraft; or
  - b) was committed outside the national territory of the deciding State, whenever, according to Austrian law, offences of that type committed outside the national territory would not come under the scope of Austrian criminal laws,
3. if a final and enforceable decision in Austria or a final and already enforced decision in another State was issued against the person concerned for the offence underlying the decision,
4. if the offence underlying the decision is punishable neither by a court nor as an administrative offence pursuant to Austrian law, unless the offence can be assigned to one of the categories of punishable offences and administrative offences that are listed in Annex 1, Part A or Part B; the classification made by the deciding State shall be binding with the proviso of § 53c (3) item 3;
5. if the offence underlying the decision was committed by a person who was below the age of criminal responsibility under Austrian law at the time of the offence,
6. if enforcement of the offence underlying the decision, which comes under the scope of Austrian criminal law, has become time-barred pursuant to Austrian law;
7. if the person concerned has been granted amnesty or has been pardoned in Austria or the deciding State;
8. whenever enforcement were to violate provisions on immunity,
9. if the decision was issued in written proceedings and the person concerned was not informed in person or through a representative authorized under the law of the deciding State of the possible and existing legal remedies and the deadlines applicable to them,
10. if the decision was taken in the absence of the person concerned, unless he/she was informed in person or through a representative authorized under the law of the deciding State of the proceedings or stated that he/she will not challenge the decision;
11. if there are objective indications that, when taking the decision, fundamental rights or essential legal principles, as defined in Article 6 of the Treaty on European Union were violated, especially pecuniary sanctions for the purpose of punishing the person concerned for reasons of his/her sex, race, religion, ethnic origin, nationality, language, political conviction or sexual orientation, and if the person concerned did not have any possibility to claim these circumstances before the European Court of Human Rights or before the European Court of Justice.

### **Competences**

**§ 53b.** (1) The regional court with subject-matter competences is the competent authority to decide on the execution of a decision imposing a pecuniary sanction.

(2) The venue shall be determined by the domicile or the residence of the person who is the subject of the pecuniary sanction; in the event of an association (§ 1 (2) and (3) of the VbVG), venue shall be determined by the registered office or the place of operation or the residence of the association. If these locations cannot be determined, the place shall be decisive where the assets are located concerning which the decision is to be executed. If the competences of a specific court cannot be determined on the basis of the present provisions, the Regional Court for Criminal Matters Vienna shall have jurisdiction.

(3) If the court that has been seized with an execution is not the competent authority, it shall transfer the matter to the competent court.

(4) If the decision imposing a pecuniary sanction is not a decision pursuant to § 53 (1) or (2), the matter shall be transferred to the competent district administrative authority or federal police directorate.

### **Procedure**

**§ 53c.** (1) Execution shall require that

1. the decision to be executed and
2. the certificate (**Annex VI**), signed by the competent authority, and – in the event that the deciding State did not make any statement that, as an executing State, it will also accept certificates in German (§ 53k (2)) – its translation into the German language

is communicated to the Austrian court.

(2) If the authority of the deciding State has classified the underlying criminal offence as belonging to the categories indicated in Annex I, Part B, item 7, the certificate shall contain the detailed circumstances of the offence, the applied domestic legal provisions and that provision of the legal act issued on the basis of the Treaty establishing the European Communities or the Treaty on European Union, which are transposed by domestic legal stipulations.

(3) If

1. the certificate was not communicated, is incomplete in essential sections, or obviously contradicts the decision,
2. there are indications that one of the reasons applies which are listed in § 53a, items 6, 9, 10 and 11, rendering execution inadmissible,
3. the legal classification as an offence pursuant to Annex I, Part A or B is obviously erroneous, or the person concerned has raised justified objections against it, or
4. the person concerned documents that the pecuniary sanction has been paid or collected in full or in part,

the authority of the deciding State shall be requested to subsequently submit the certificate, to complete it or to provide supplementing information, for which acts a reasonable period of time shall be set, together with the indication that execution will be refused in full or in part if the period of time expires without any reaction.

(4) § 14 (1) to (5) shall be applied in analogy to the exchanges between the authorities.

(5) The person concerned shall be heard on the requirements for execution (§ 53, § 53a), on the amount of the sum to be executed (§ 53d (2)), and on the amount of the daily rates applicable to the prison term in lieu of payment, if they have not yet been determined in the decision to be executed, if he/she can be summoned in Austria.

### **Decision**

**§ 53d.** (1) A decision shall be taken on execution. The decision shall indicate the name of the authority, the decision of which is to be executed, its file number, a short statement of the facts, including the time and place

of the offence, the name of the punishable offence, as well as the legal provisions of the deciding State that were applied.

(2) If execution is accepted, the amount to be executed in Austria shall be fixed as that amount which was imposed by the decision to be executed. If the amount is not in euros, it shall be converted, using the exchange rate applicable on the day on which the decision on execution is taken. However, the amount to be executed shall be reduced to the maximum amount admissible under Austrian law, if the offence underlying the decision was committed outside the national territory of the deciding State and comes under the scope of application of the Austrian criminal law. Previously made payments and collected amounts shall be taken into account.

(3) If the prison term in lieu of payment of the fine has not already been fixed in the decision to be executed, which imposes a financial penalty, but if the certificate indicates that imprisonment in lieu of payment of the fine is admissible pursuant to the law of the deciding State, an prison term in lieu of payment of the fine shall be fixed in the decision on execution for the event that the financial penalty cannot be collected. The prison term shall be determined by the period of time that corresponds to the number of daily rates (§ 19 (3) of the Austrian Criminal Law Code) which would have to be fixed for the offence according to Austrian law, or which otherwise would have to be fixed in keeping with Austrian law, but it must not exceed any maximum period of time indicated in the certificate.

(4) The public prosecutor and the person concerned shall have the right to filing a complaint against the decision to the higher regional court within 14 days. A complaint by the person concerned, which is filed in time, has suspensive effect.

(5) § 409 of the Code of Criminal Procedure shall be applied once the decision has become final and enforceable.

(6) If execution was refused on account of the reason given in § 53am item 11, the competent public prosecutor shall report this to the Federal Ministry of Justice, attaching a copy of the decision.

#### **Postponing Execution**

§ 53e. (1) The execution of a decision which imposes a pecuniary sanction shall be postponed

1. as long as no final and enforceable decision has been taken on an admissible complaint (§ 53d (4));
2. for the period of time which the court deems necessary in order to produce a translation of the decision at the court's costs;
3. until the supplementary information requested from the authority of the deciding State has been received.

(2) During the period of the deferral all admissible measures shall be taken in order to prevent that the amount of money to be collected is no longer available for the purpose of executing the decision, once the reason for the deferral no longer applies.

#### **Proceeds from Execution**

§ 53f. The proceeds from execution shall accrue to the Federal State, unless an arrangement to a different effect has been reached with the deciding State.

#### **Imprisonment in lieu of a Pecuniary Sanction**

§ 53g. If a financial penalty cannot be collected, enforcement of the imprisonment in lieu of payment of the fine shall be ordered, which has been fixed in the decision to be executed or in the decision on execution (§ 53d (3)).

#### **Discontinuing Execution**

§ 53h. If the competent authority of the deciding State communicates that the decision imposing a pecuniary sanction or its enforceability have been lifted, or that execution is no longer requested for some other reason, execution shall be discontinued.

### **Informing the Deciding State**

- § 53i.** The court shall immediately bring to the attention of the competent authority of the deciding State if
1. it transfers the matter to the competent court or the competent territorial administrative authority or police directorate (§ 53b (3) and (4)),
  2. the amount to be executed is lower than the amount fixed in the decision (§ 53d (2)),
  3. a prison term in lieu of payment of the fine is fixed and its enforcement is ordered (§ 53g),
  4. a decision has been executed,
  5. execution is denied in full or in part, indicating the reasons,
  6. the decision cannot be executed in Austria due to reasons of uncollectability.

### **Costs**

**§ 53j.** The costs accruing when executing a foreign decision imposing a pecuniary sanction shall be borne by the Federal State, irrespective of whether they can be collected from the person concerned or not.

### **Subdivision Two: Obtaining Execution in Another Member State**

#### **Seizing Another Member State**

**§ 53k.** (1) If there are reasons to seize another Member State with the execution of a court decision which imposed a pecuniary sanction (§ 53 (2)), the regional court shall first afford the public prosecutor the opportunity to comment and to hear the person concerned, if he/she can be summoned in Austria.

(2) The court shall communicate to the competent authority of the executing State

1. the decision to be executed, complete with a translation, if such a translation was already made for the foreign person concerned in the proceedings in Austria, as well as a completed and signed certificate (**Annex VI**) and, unless the executing State indicated that it also accepts certificates in the German language, a translation of the certificate into one of the official languages of the executing State or into another language accepted by it.

The Federal Minister of Justice shall proclaim by way of ordinance which Member States accept which official languages.

(3) § 14 (1) to (5) shall apply in analogy to the exchanges between the authorities. If the decision and the certificate were not communicated by mail, the competent authority of the executing State shall subsequently be sent by mail, upon its request, a specimen or a certified copy of the decision, as well as the original of the certificate.

(4) It shall be inadmissible to seize one further Member State with the execution at the same time.

#### **Revoking Seizure of Member State**

**§ 53l.** The court shall immediately inform the competent authority of the executing state if

1. the person concerned already paid an amount of money as a result of the decision which imposed the pecuniary sanction,
2. the decision imposing the pecuniary sanction or its enforceability are subsequently lifted, modified, or the amount of the pecuniary sanction is reduced, or
3. execution is no longer requested for other reasons.

#### **Execution in Austria.**

**§ 53m.** (1) If a Member State was seized with execution, it shall be inadmissible to conduct an execution in Austria.

(2) However, the execution procedure may be continued

1. after the competent authority of the executing State has been informed that execution is no longer requested,
2. if a pardon or amnesty in the executing State has resulted in the discontinuation of execution,
3. if execution in the executing State is not possible in the absence of collectability, or
4. if the executing State refuses execution, unless the refusal was supported by the reason listed in § 53a, item 3.

#### **Execution of Foreign Fines**

**§ 53.** (1) § 64 to § 67 of the ARHG shall apply to the execution of fines that were imposed with final and enforceable effect by another Member State.

(2) A request by a Member state for execution of a fine that was imposed with final and enforceable effect may only be executed if it is ensured that the requesting Member State would comply with a similar Austrian request, or if conventions under international law require the execution of such fines. Moreover, § 3 of the ARHG shall apply in analogy.

## **PolK Police Cooperation Act**

### **Scope of Application**

**Section 1** (1) International cooperation serves the purposes of

1. law enforcement (police),
2. CID (Criminal Investigation Division),
3. passport authorities, Aliens Police, and border control.

(2) International Police Cooperation comprises

1. international mutual assistance in police matters
2. intervention by law enforcement authorities and their officers abroad, and law enforcement authorities of other countries and their officers in Austria, especially in form of hot pursuit and cross-border surveillance.

(3) Request for and execution of Letters Rogatory pursuant to the Extradition and Legal Assistance Act, Federal Law Gazette No. 529/1979 or bilateral agreements remain unaffected.

### **Tasks**

**Section 3** (1) The law enforcement authorities are obliged to render legal assistance upon request

1. pursuant to international law,
2. if it serves to fulfil the duties stipulated under s.1, para.1, of a foreign law enforcement authority on condition of reciprocity, or
3. if required by a law enforcement organisation for task fulfilment as outlined under s1, p.1.

(2) The law enforcement authorities are obliged to render legal assistance also without being requested,

1. by using data that have – owing to their nature – to be transmitted under international law, or
2. if required by a foreign law enforcement authority for the purpose of fulfilling its duties pursuant to s.1, p.1, on condition of reciprocity,
3. if required for criminal investigation activities by Interpol.

### **Fulfilment of Tasks**

**Section 5** (1) The law enforcement authorities are empowered to provide legal assistance

1. in form of any measure that does not interfere with the rights of a human being, or
2. by using person-related data in conformity with the following paragraphs and Section 3.

(2) If binding international law does not otherwise indicate, interfering with rights of a person is admitted for the purpose of legal assistance as far as this would be legal in a comparable case within the jurisdiction of an Austrian law enforcement authority; such interferences have to be in compliance with national procedural standards.

(3) Establishing data for the purpose of rendering legal assistance is admissible by

1. using data established by the authority itself in enforcing a federal or provincial law,
2. requesting information from other law enforcement authorities,
3. requesting information from services of territorial or local authorities or corporations under public law, institutions operated by them and operators of public telecommunication services, in conformity with s. 53, para. 3a, of the Austrian Code of Police Practice,

4. interviewing persons who when made aware of the official nature of the interview volunteer to provide information ('overt interview'),
  5. surveillance, if this constitutes a vital precondition to effectively render legal assistance.
- (4) As regards overt interview and surveillance by law enforcement officers, officers of foreign law enforcement authorities may be present with the consent of the Federal Ministry of the Interior, if required to fulfil tasks according to s.1, para. 1, and upon reciprocity. In such a case, the interviewee has to be made aware of the presence of the officers of the foreign law enforcement authority.
- (5) The Federal Ministry of the Interior is authorized to instruct also other law enforcement authorities with establishing data as outlined under paragraph 3, sub-paragraphs 3 to 5. As regards transmission to another law enforcement organisation or a foreign law enforcement authority, this is admissible only if the nature of the data in question have been established with certainty.

### **Request for Legal Assistance**

#### ***Principle***

**Section 6** The law enforcement authorities are empowered to request legal assistance for fulfilling the tasks outlined in s. 1, para 1. They may only request measures which they themselves are authorized to take in fulfilling the task underlying the request. Foreign law enforcement authorities in charge of making risk assessments only, may not be asked for legal assistance in criminal investigations.

## **SPG Security Police Act**

### **Federal Minister of the Interior**

**Article 6.** (1) The organisational units of the Federal Ministry of the Interior managing matters of security administration shall form the General Headquarters for Public Security [Generaldirektion für die öffentliche Sicherheit]. Establishment and organisational set-up of the Federal Office of Criminal Investigation [Bundeskriminalamt] as an organisational unit of the General Headquarters for Public Security shall be governed by a special federal act.

(2) Public security service officers assigned or allocated to the General Headquarters for Public Security shall provide police services for the Federal Minister of the Interior.

(3) In agreement with the Executive Committee of the National Council [Nationalrat], by ordinance, for purposes of a more efficient fight against criminal associations, or if special training is required therefore due to the coercive measures which may have to be taken against persons and objects to terminate dangerous attacks, the Federal Minister of the Interior shall be entitled to form special units from among officers under para (2) and charge them with exclusive or focussed performance of these tasks in the entire federal territory. This shall not apply to special units having already existed prior to 1 July 1997.

.../...

### **Definition of Terms General Danger; Dangerous Attack; Potential Danger Identification**

**Article 16.** (1) “General danger“ shall be imminent

1. in a dangerous attack (paras (2) and (3)) or
2. as soon as three or more people collaborate with the intent to continue to commit punishable acts (criminal association).

(2) A “dangerous attack“ shall be the threat posed to a legal interest by the illegal realisation of the elements of a judicially punishable act which is committed intentionally and is prosecuted not only at the request of a person involved if it is a criminal offence

1. under the Criminal Code (CC - StGB), FLG No. 60/1974, except for offences under art. 278, 278a and 278b StGB, or
2. under the Act Banning the NSDAP and Forbidding Nazi Activity (Verbotsgesetz), StGBI. No. 13/1945, or
3. under the 2005 Aliens' Police Act (Fremdenpolizeigesetz 2005 - FPG), FLG I No. 100, or
4. under the Addictive Drugs Act (Suchtmittelgesetz - SMG), FLG I No. 112/1997, except for acquisition or possession of narcotic drugs for personal use.

(3) A “dangerous attack“ shall also be conduct aimed at and appropriate to preparing such threat (para (2)) if this conduct is exhibited in close relationship as to time with the intended realisation of the offence.

(4) “Potential danger identification“ shall be the isolation of the source of danger and the facts otherwise relevant to danger aversion.

## BWG Banking Act

### **X. Due Diligence Obligations, Suppression of Money Laundering and of Terrorist Financing** **General Due Diligence Obligations**

**Article 39.** (1) In their management activities, the managers of a credit institution must exercise the diligence of a prudent and conscientious manager as defined in Article 84 para. 1 of the Stock Corporation Act. In particular, they must obtain information on and control, monitor and limit the risks of banking transactions and banking operations using appropriate strategies and mechanisms, and have in place plans and procedures pursuant to Article 39a. Moreover, they must consider the overall earnings situation of the credit institution.

(2) Credit institutions must have in place administrative, accounting and control mechanisms for the capture, assessment, management and monitoring of risks arising from banking transactions and banking operations. These mechanisms must be appropriate to the type, scope and complexity of the banking transactions conducted. Wherever possible, the administrative, accounting and control procedures must also capture risks arising from banking transactions and banking operations which might possibly arise. The organisational structure must prevent conflicts of interest and of competences by establishing delineations in structural and process organisation which are appropriate to the credit institution's business operations. The adequacy of these procedures and their enforcement must be reviewed by the internal audit unit at least once per year.

(2a) Credit institutions may make use of joint risk classification organisations as service providers for the development and ongoing maintenance of rating methods if the credit institutions report this to the FMA in advance. The participating credit institutions may convey all information necessary for the capture and assessment of risks to the joint risk classification organisation for the exclusive purpose of developing and maintaining risk assessment and mitigation methods and making these methods available to the participating credit institutions by processing the data; the risk classification organisation shall only be permitted to transfer personal data to the credit institution which originally provided the underlying borrower data. The joint risk classification organisation, its governing bodies, employees and other persons working for the organisation shall be subject to the banking secrecy requirements pursuant to Article 38. With regard to the risk classification organisation, the FMA shall have all information, presentation and auditing powers set forth in Article 70 para. 1; Article 71 is applicable in this context.

(2b) In particular, the procedures pursuant to para. 2 must include the following:

1. credit risk (Article 2 no. 57),
2. concentration risk (Article 2 no. 57b),
3. risk types in the trading book (Article 22o para. 2),
4. commodities risk and foreign exchange risk, including the risk arising from gold positions, where these are not covered by no. 3,
5. operational risk (Article 2 no. 57d),
6. securitisation risk (Article 2 no. 57c),
7. liquidity risk (Article 25),
8. interest rate risk arising from any transactions not already covered by no. 3,
9. the residual risk from credit risk mitigation techniques (Article 2 no. 57a) and
10. risks arising from the macroeconomic environment.

(2c) In the case of new transactions with which the credit institution has no experience regarding the risks involved, due consideration must be given to the security of third-party funds entrusted to the credit institution and to the preservation of the credit institution's own funds. The procedures pursuant to para. 2 must ensure that

the risks arising from new transactions as well as concentration risks are captured and assessed to the fullest possible extent.

(3) *removed (Federal Law Gazette I No. 108/2007)*

(4) Credit institutions which apply Article 22o must ensure that

1. the risk positions in the trading book can be calculated at any time;
2. where internal models are applied, the documentation is prepared in a transparent manner and enables trials using test cases; and
3. the bank auditor and auditors pursuant to Article 70 para. 1 no. 3 can review the calculation of risk positions in the trading book at any time.

### **Internal Capital Adequacy Assessment Process**

**Article 39a.** (1) Credit institutions must have in place effective plans and procedures in order to determine on a regular basis the amount, the composition and the distribution of capital available for the quantitative and qualitative coverage of all material risks from banking transactions and banking operations and to hold capital in the amount necessary. These plans and procedures must be based on the nature, scope and complexity of the banking transactions conducted.

(2) Credit institutions must review the suitability and enforcement of the strategies and procedures pursuant to para. 1 at regular intervals, in any case on an annual basis, and to adapt those strategies and procedures as necessary.

(3) The superordinate credit institution is to fulfil the obligations under para. 1 exclusively on a consolidated basis. Where a financial holding company established in Austria is superordinate to a group of credit institutions, the consolidated financial situation of the financial holding company is to be used as the basis.

(4) Subordinate credit institutions as defined in Article 30 paras. 1 and 2 whose superordinate credit institution complies with the requirements pursuant to paras. 1 to 2 on the basis of its consolidated financial position are not required to comply with paras. 1 and 2.

(5) By way of derogation from paras. 3 and 4, subordinate credit institutions must comply with paras. 1 and 2 exclusively on a subconsolidated basis if they have as subsidiary undertakings credit institutions, financial institutions or asset management companies incorporated in third countries as defined in Article 2 (5) of Directive 2002/87/EC.

### **X. Due Diligence Obligations for the Suppression of Money Laundering and of Terrorist Financing**

**Article 40.** (1) Credit institutions and financial institutions must ascertain and verify the identity of a customer:

1. before initiating a permanent business relationship; savings deposit transactions pursuant to Article 31 para. 1 of this federal act and transactions pursuant to Article 12 of the Depository Act (*Depotgesetz – DepotG*) are always considered to be permanent business relationships;
2. before executing any transactions which are not conducted in connection within a permanent business relationship and which involve an amount of at least EUR 15,000 or an equivalent value, regardless of whether the transaction is carried out in a single operation or in multiple operations between which there is an obvious connection; in cases where the amount is unknown at the beginning of a transaction, the identity of the customer must be ascertained as soon as the amount is known and it is determined that it will come to at least EUR 15,000 or an equivalent value;
3. if the institution suspects or has reasonable grounds to suspect that the customer belongs to a terrorist organisation (Article 278b StGB) or the customer objectively participates in transactions which serve the purpose of money laundering (Article 165 StGB – including asset components which

stem directly from a criminal act on the part of the perpetrator) or terrorist financing (Article 278d StGB).

4. after 31 October 2000 for each deposit into savings deposits, and after 30 June 2002 also for each withdrawal of savings deposits if the amount deposited or withdrawn comes to at least EUR 15,000 or an equivalent value;

5. when there are doubts as to the veracity or adequacy of previously obtained customer identification data.

The identity of a customer is to be ascertained by the personal presentation of an official photo identification document by the customer. For the purposes of this provision, documents which are issued by a government authority and which bear a non-replaceable, recognisable photograph of the head of the person in question and include the name, date of birth and signature of the person as well as the authority which issued the document are considered to be official photo identification documents; in the case of foreign passports, the passport need not contain the person's complete date of birth if this complies with the law of the country which issued the passport. In the case of legal persons and natural persons who are not legally competent, the identity of the natural person authorised to represent the former is to be verified by presentation of the latter's official photo identification document and the power of representation is to be verified by means of suitable documents. The identity of the legal person must be ascertained on the basis of meaningful supporting documentation which is available under the usual legal standards of the country in which the legal person is incorporated. Exceptions to the provisions above may only be made in the cases pursuant to para. 8 and Article 40a. Individual criteria with regard to the official photo identification may be waived where technical advances, such as biometric data, give rise to other criteria which are at least equivalent to the waived criteria in terms of their identification effects. However, the criterion stipulating that the identification must be issued by a government authority must always be fulfilled.

(2) Credit institutions and financial institutions must call upon the customer to indicate whether he/she intends to conduct the business relationship (para. 1 no. 1) or the transaction (para. 1 no. 2) for his/her own account, or for the account of or on behalf of a third party; the customer must comply with this request. If the customer indicates that he/she intends to conduct the business relationship (para. 1 no. 1) or the transaction (para. 1 no. 2) for the account of or on behalf of a third party, the customer must provide the credit institution or financial institution with evidence of the trustor's identity. The identity of the trustee must be ascertained in accordance with para. 1 and exclusively in the physical presence of the trustee. The identity of the trustee may not be ascertained by third parties. The identity of the trustor is to be evidenced by the presentation of the original or a copy of the trustor's official photo identification document (para. 1) in the case of natural persons and by the presentation of meaningful supporting documentation pursuant to para. 1 in the case of legal persons. The trustee must also submit a written declaration to the credit institution or financial institution stating that the trustee has ascertained the identity of the trustor personally or through reliable sources. In this context, reliable sources refer to courts and other government authorities, notaries, attorneys at law, and third parties as specified in para. 8. In the case of special fiduciary accounts of authorised real estate administrators acting on behalf of joint ownership associations for real estate properties, the presentation of an excerpt from the property register is considered valid evidence of the trustors' identity in the case of joint owners who are natural persons.

(2a) Credit institutions and financial institutions must also:

1. call upon the customer to reveal the identity of the customer's beneficial owner; the customer must comply with this request, and credit institutions and financial institutions must take risk based and appropriate measures to verify the beneficial owner's identity so that the credit institution or financial institution is satisfied that it knows who the beneficial owner is; in the case of legal persons or trusts, this also includes taking risk-based and appropriate measures in order to understand the ownership and control structure of the customer;

2. take risk-based and appropriate measures to obtain information on the purpose and nature of the intended business relationship;

3. take risk-based and appropriate measures to conduct ongoing monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of that relationship, to ensure that the transactions conducted are consistent with the institutions' knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds, and to ensure that the documents, data or information held are kept up to date.

(2b) Credit institutions and financial institutions must subject their business to risk analysis using suitable criteria (in particular products, customers, the complexity of transactions, customer business and geography) with regard to the risk of misuse for the purposes of money laundering and terrorist financing. Credit institutions and financial institutions must be able to demonstrate to the FMA that the extent of the measures taken on the basis of the analysis is appropriate in view of the risks of money laundering and terrorist financing.

(2c) By way of derogation from paras. 1, 2 and 2a, the opening of a bank account is permissible provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on the customer's behalf until full compliance with paras. 1, 2 and 2a regarding customer identification and the other required information on the business relationship has been attained.

(2d) In cases where credit institutions and financial institutions are not in a position to comply with paras. 1, 2 and 2a regarding customer identification and the other required information on the business relationship, they must not carry out any transaction or establish a business relationship, or they must terminate the business relationship; moreover, the credit institution or financial institution must consider reporting the customer to the relevant authorities (Article 6 Security Police Act) in accordance with Article 41 para. 1.

(2e) Credit institutions and financial institutions must apply the due diligence obligations regarding the ascertainment and verification of the customer's identity pursuant to Articles 40 et seq. not only to all new customers, but also to existing customers on a risk-sensitive basis at the appropriate times.

(3) Credit institutions and financial institutions must retain the following:

1. documents serving the purpose of identification pursuant to paras. 1, 2, 2a and 2e for at least five years after the termination of the business relationship with that customer;
2. documentation and records of all transactions for a period of at least five years after their execution.

(4) Credit institutions and financial institutions must

1. ensure that the measures applied at their branches and subsidiaries located in third countries are at least equivalent to those set forth in this federal act with regard to customer due diligence and record-keeping;
2. inform the FMA in cases where the legislation of the third country does not permit application of the measures required under no. 1, and take additional measures to handle the risk of money laundering or terrorist financing effectively.

The FMA must inform the competent authorities of the other Member States and the European Commission of cases where the legislation of a third country does not permit application of the measures required under no. 1 and coordinated action could be taken to pursue a solution.

(5) The acceptance and acquisition of securities for

1. securities accounts (Article 11 Depository Act) and
2. business relationships pursuant to Article 12 Depository Act which were initiated or entered into before 1 August 1996, are only permissible if the identity of the customer has first been ascertained and the requirements of para. 2 and 2a have been fulfilled.

The sale of securities and the withdrawal of balances and income from securities accounts (Article 11 Depository Act) and from business relationships pursuant to Article 12 Depository Act may only be carried out

after 30 June 2002 if the identity of the customer has first been ascertained and the requirements of para. 2 and 2a have been fulfilled.

(6) Deposits into existing savings accounts pursuant to Article 31 may not be effected or accepted if the customer's identity has not been ascertained in accordance with para. 1. Likewise, funds transfers must not be credited to such savings accounts if the customer's identity has not been ascertained in accordance with para. 1.

(7) After 30 June 2002, savings accounts for which the customer's identity has not been ascertained pursuant to para. 1 must be maintained as specially labelled accounts. Deposits into and withdrawals from those accounts may not be made, and funds transfers may not be credited to those accounts until the customer's identity has been ascertained pursuant to para. 1.

(8) Credit institutions and financial institutions may rely on third parties in order to fulfil the obligations set forth in Article 40 paras. 1, 2 and 2a nos. 1 and 2. However, the ultimate responsibility for fulfilling those obligations remains with the credit institutions or financial institutions which rely on third parties. For the purposes of this paragraph, third parties are considered to be the following unless they are authorised exclusively to carry out exchange bureau business (Article 1 para. 1 no. 22) or remittance services business (Article 1 para. 1 no. 23):

1. the credit institutions and financial institutions indicated in Article 3 (1) and (2) of Directive 2005/60/EC;
2. the credit institutions and financial institutions indicated in Article 3 (1) and (2) of Directive 2005/60/EC and located in a third country; and
3. the persons indicated in Article 2 (1) (3) (a) and (b) of Directive 2005/60/EC, in each case subject to the requirement that they are subject to mandatory professional registration recognised by law and must apply customer due diligence requirements and record-keeping requirements as set forth in or equivalent to those set forth in Articles 40 et seq. or Directive 2005/60/EC, and their compliance with those requirements is supervised in accordance with Section 2 of Chapter V of that Directive, or they are situated in a third country which imposes equivalent requirements to those laid down in that Directive. The FMA must inform the competent authorities of the other Member States and the European Commission of cases in which the FMA considers that a third country fulfils the conditions set forth above. Where the European Commission adopts a decision pursuant to Article 40 (4) of Directive 2005/60/EC, the Austrian federal government will, in agreement with the Main Committee of the National Council, issue a regulation prohibiting credit institutions and financial institutions from relying on third parties from the third country in question for the purpose of fulfilling the obligations set forth in paras. 1, 2 and 2a nos. 1 and 2. Credit institutions and financial institutions must ensure that the third parties make the information required to fulfil the obligations set forth in paras. 1, 2, para. 2a nos. 1 and 2, and in Article 8 (1) (a) to (c) of Directive 2005/60/EC available to them without delay. Moreover, credit institutions and financial institutions must ensure that the relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner is forwarded immediately at the credit institution's or financial institution's request. This paragraph does not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the credit institution or financial institution obliged to fulfil the obligations set forth in paras. 1, 2 and 2a nos. 1 and 2.

(9) removed (*Federal Law Gazette I No. 108/2007*)

#### **Simplified Customer Due Diligence Obligations**

**Article 40a.** (1) By way of derogation from Article 40 para. 1 nos. 1, 2 and 5, and paras. 2 and 2a, the obligations indicated in those provisions do not apply in cases where the customer is a credit institution or financial institution pursuant to Article 1 paras. 1 and 2 or pursuant to Article 3 of Directive 2005/60/EC, or a

credit institution or financial institution situated in a third country which imposes obligations equivalent to those set forth in Directive 2005/60/EC and supervised for compliance with such obligations.

(2) By way of derogation from Article 40 para. 1 nos. 1, 2 and 5, and paras. 2 and 2a, the obligations indicated in those provisions do not apply provided that the risk of money laundering and terrorist financing is considered low in accordance with para. 4 if the customer(s) is (are):

1. exchange-listed companies whose securities are admitted to listing on a regulated market in one or more Member States, or exchange-listed companies from third countries which are subject to disclosure obligations pursuant to a regulation to be issued by the FMA on the basis of its power to issue regulations pursuant to Article 85 para. 10 Stock Exchange Act and such disclosure obligations are equivalent or comparable to those set forth in Community legislation;
2. domestic authorities; or
3. authorities or public bodies
  - a) if they are entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation;
  - b) the identity of which is publicly available, transparent and certain;
  - c) the activities and accounting practices of which are transparent; and
  - d) if they are accountable either to a Community institution or to the authorities of a Member State, or appropriate check and balance procedures exist ensuring control of the customer's activity.

(3) Para. 2 also applies to:

1. customers with regard to electronic money (Article 2 no. 58) where, if the device cannot be recharged, the amount stored in the device is no more than EUR 150, or where, if the data medium can be recharged – a limit of EUR 2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1,000 or more is redeemed in the same calendar year by the bearer pursuant to Article 6 E-Money Act or pursuant to Article 3 of Directive 2000/46/EC;
2. savings activities for classes of school pupils, subject to the condition that the cooperation of the legal representative is not required in the identification of the school pupil and that, unless Article 40 para. 1, 2 or 2a is applied in its entirety,
  - a) in the case of savings passbook accounts which are opened for individual minors, identification can be performed by the school pupil himself/herself in the presence of a teacher or through a teacher as a trustee; the identification data of the school pupils can be ascertained by the credit institution on the basis of their school identification cards, copies of their school identification cards or a list containing the names, dates of birth and addresses of the pupils in question;
  - b) in the case of collective savings passbooks for school classes, the identification of the minor school pupils entitled to the savings deposit can be performed by a teacher as a trustee using a list containing the names, dates of birth and addresses of the pupils in question.

(4) In assessing whether the customers or products and transactions indicated in paras. 2 and 3 represent a low risk of money laundering or terrorist financing, credit institutions and financial institutions must pay special attention to the activities of such customers and to the types of products and transactions which may be regarded as particularly likely, by nature, to be used or abused for money laundering or terrorist financing purposes. Credit institutions and financial institutions must not consider that the customers or products and transactions indicated in paras. 2 and 3 represent a low risk of money laundering or terrorist financing if there is information available to suggest that the risk of money laundering or terrorist financing may not be low.

(5) By way of derogation from Article 40 paras. 1, 2 and para. 2a nos. 1 and 2, in the case of fiduciary accounts held by attorneys at law or notaries, including those from Member States or third countries as long as they are

subject to requirements equivalent to international standards with regard to the suppression of money laundering or terrorist financing and are supervised for compliance with such requirements, evidence of the identity of each individual trustor need not be provided to the credit institution or financial institution if the following requirements are fulfilled:

1. individual verification is infeasible due to the representation of large co-ownership communities of changing composition;
2. the trustee submits a written declaration to the credit institution stating that he/she has identified his/her clients in accordance with Article 40 paras. 1, 2 and para. 2a nos. 1 and 2 or the requirements of Directive 2005/60/EC, that he/she has stored the corresponding documents and will present them to the credit institution upon request; this does not apply to clients for whom the respective individual transaction conducted or whose share of the claim on the respective trustee arising from fiduciary accounts does not amount to a total of EUR 15,000;
3. the trustee provides the credit institution with complete lists of the clients assigned to each fiduciary account within two months after the end of each calendar quarter; this does not apply to clients for whom the respective individual transaction conducted or whose share of the claim on the respective trustee arising from fiduciary accounts does not amount to a total of EUR 15,000;
4. the trustor does not have his/her place of incorporation or place of residence in a noncooperative country or territory; and
5. no suspicion pursuant to Article 40 para. 1 no. 3 exists.

(6) Credit institutions and financial institutions must retain sufficient information in order to demonstrate that the customer is eligible for exemption in accordance with paras. 1 to 5.

(7) In agreement with the Main Committee of the Austrian National Council, the Austrian federal government must issue a regulation stating that the exemptions pursuant to para. 1, 2 or 5 are not longer applicable if the European Commission adopts a decision pursuant to Article 40 (4) of Directive 2005/60/EC.

(8) The FMA must inform the competent authorities of the other Member States and the European Commission of cases where the FMA considers that a third country fulfils the conditions set forth in para. 1, 2 or 5.

### **Enhanced Customer Due Diligence Obligations**

**Article 40b.** (1) In situations which by their nature can present a higher risk of money laundering or terrorist financing, credit institutions and financial institutions must apply additional due diligence measures in addition to the obligations pursuant to Article 40 paras. 1, 2, 2a and 2e on a risk-sensitive basis. In any event, credit institutions and financial institutions must take the following additional measures:

1. in cases where the customer or the natural person authorised to represent the person pursuant to Article 40 para. 1 is not physically present for identification purposes and thus the presentation of an official photo identification in person is not possible, credit institutions and financial institutions must take specific and adequate measures to compensate for the increased risk; except in cases of suspicion or reasonable grounds for suspicion pursuant to Article 40 para. 1 no. 3, as in such cases business relations must be avoided in any event, credit institutions and financial institutions must at least ensure that:

either

- a) the contractual declaration of the customer is either submitted electronically using a secure electronic signature pursuant to Article 2 no. 3 Signatures Act (*Signaturgesetz – SigG*; Federal Law Gazette I No. 190/1999); or, if this is not the case, the contractual declaration of the credit

institution or financial institution is delivered in writing by registered mail to that customer address which is indicated as the customer's place of residence or place of incorporation;

b) the customer's name, date of birth and address in the case of natural persons, or the company name and place of incorporation in the case of legal persons, are known to the credit institution or financial institution; in the case of legal persons, the place of incorporation must also be the seat of the undertaking's central administration, which must be confirmed by the customer in a written declaration; a copy of the official photo identification document of the customer or of the customer's legal representative, or of the authorised representative in the case of legal persons, is also submitted to the credit institution or financial institution before the time of conclusion of the agreement, unless the legal transaction is concluded electronically using a secure electronic signature; and

c) if the customer's place of incorporation or place of residence is outside the EEA, then a written declaration is required from another credit institution with which the customer has a permanent business relationship, stating that the customer has been identified in accordance with Article 40 paras. 1, 2 and 2a nos. 1 and 2, or Article 8 (1) (a) to (c) of Directive 2005/60/EC, and that the permanent business relationship is still maintained. If the credit institution providing the confirmation is incorporated in a third country, then this third country must impose requirements which are equivalent to those indicated in Articles 16 to 18 of the directive mentioned above. In lieu of identification and confirmation by a credit institution, identification and written confirmation by the Austrian representation in the third country in question or by a recognised certification authority is also permissible;

or

d) the first payment of the operations is carried out through an account opened in the customer's name with a credit institution as specified in Article 40 para. 8; in such cases, however, the customer's name, date of birth and address in the case of natural persons, or the company name and place of incorporation in the case of legal persons must be known to the credit institution or financial institution, and the credit institution or financial institution must have at its disposal copies of customer documents on the basis of which the information provided by the customer or the natural person authorised to represent the customer can be verified in a credible manner. In lieu of such copies, a written declaration stating that the customer has been identified in accordance with Article 40 paras. 1, 2, 2a and 2e, or Article 8 (1) (a) to (c) of Directive 2005/60/EC from the credit institution through which the first payment is to be carried out will be considered sufficient.

2. with regard to cross-border correspondent banking relationships with correspondent banks from third countries:

a) credit institutions and financial institutions must gather sufficient information about a correspondent bank to understand fully the nature of its business and be able to ascertain the reputation of the institution and the quality of supervision on the basis of publicly available information;

b) credit institutions and financial institutions must satisfy themselves of the correspondent bank's anti-money laundering and anti-terrorist financing controls;

c) credit institutions and financial institutions must obtain approval from senior management before establishing new correspondent banking relationships;

d) credit institutions and financial institutions must document the respective responsibilities of each institution;

e) with respect to payable-through accounts, credit institutions and financial institutions must be satisfied that the correspondent bank has verified the identity of and performed ongoing due

diligence on the customers having direct access to accounts of the correspondent, and that it is able to provide relevant customer due diligence data to the correspondent bank upon request;

3. with regard to transactions or business relationships to politically exposed persons from other Member States or from third countries:

- a) credit institutions and financial institutions must have appropriate risk-based procedures to determine whether the customer is a politically exposed person;
- b) credit institutions and financial institutions must obtain senior management approval before establishing business relationships with such customers;
- c) credit institutions and financial institutions must take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction; and
- d) credit institutions and financial institutions must conduct enhanced ongoing monitoring of the business relationship.

(2) Credit institutions and financial institutions must review with particular care each transaction which they regard as particularly likely, by its nature, to be related to money laundering (Article 165 StGB – including asset components which stem from a criminal act on the part of the perpetrator himself/herself) or terrorist financing (Article 278d StGB) and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

#### **Relief for Certain Transfers of Funds**

**Article 40c.** (1) Regulation (EC) No. 1781/2006 on information on the payer accompanying transfers of funds does not apply to domestic transfers of funds to a payee account permitting payments for the provision of goods or services if:

- 1. the payment service provider of the payee is subject to the obligations set forth in Directive 2005/60/EC;
- 2. the payment service provider of the payee is able by means of a unique reference number to trace back, through the payee, the transfer of funds from the natural or legal person who has an agreement with the payee for the provision of goods and services;
- 3. the amount transacted is EUR 1,000 or less.

(2) Article 5 of Regulation (EC) No. 1781/2006 on information on the payer accompanying transfers of funds does not apply to transfers of funds indicated in Article 18 of Regulation (EC) No. 1781/2006 which are transmitted within Austria by payment service providers established in Austria to organisations carrying out activities for non-profit charitable, religious, cultural, educational, social, scientific or fraternal purposes, provided those transfers of funds are limited to a maximum amount of EUR 150 per transfer. The payees in these funds transfers may only be organisations which publish annual accounts due to legal requirements or on a voluntary basis, whose last annual financial statements were granted an unqualified auditor's certificate by an external auditor, and which possess a certification from the Chamber of Professional Accountants and Tax Advisors confirming the fulfilment of these requirements.

(3) The FMA must publish on a quarterly basis a list of those payees to which funds transfers pursuant to para. 2 are exempt from the application of Article 5 of Regulation (EC) No. 1781/2006 on information on the payer accompanying transfers of funds. This list is to be compiled and updated on the basis of the corresponding quarterly notification from the Chamber of Professional Accountants and Tax Advisors to the FMA on the organisations which fulfil the requirements pursuant to para. 2 (second sentence). In addition to the names of the organisations themselves, this notification from the Chamber of Professional Accountants and Tax Advisors must also include the names of the natural persons who ultimately control the organisations and associations as well as explanatory notes on updates. The FMA must also inform the European Commission in accordance with Article 18 (2) of Regulation (EC) No. 1781/2006.

### **Inadmissible Business Relationships**

**Article 40d.** (1) Credit institutions must not enter into or continue a correspondent banking relationship with a shell bank pursuant to Article 2 no. 74 and must take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a credit institution which is known to permit its accounts to be used by a shell bank.

(2) In any case, credit institutions and financial institutions are prohibited from maintaining anonymous accounts and from accepting anonymous savings deposits; Article 40 paras. 5 to 7 are applicable in this context.

### **Reporting Requirements**

**Article 41.** (1) In cases where a credit institution or financial institution suspects or has reasonable grounds to suspect

1. that a previously conducted, ongoing or upcoming transaction serves the purpose of money laundering (Article 165 StGB – including asset components which stem directly from a criminal act on the part of the perpetrator); or
2. that a customer has violated the obligation to disclose fiduciary relationships pursuant to Article 40 para. 2; or
3. that a customer belongs to a terrorist organisation pursuant to Article 278b StGB or that the transaction serves the purpose of terrorist financing pursuant to Article 278d StGB, then credit institutions and financial institutions must report such suspicions to the relevant authority (Article 6 Security Police Act [*Sicherheitspolizeigesetz – SPG*]) without delay and to refrain from any further execution of the transaction until the matter is resolved, unless the danger exists that a delay in the transaction may complicate or prevent the investigation of the case. In cases of doubt, orders involving incoming funds may be executed, while orders involving outgoing funds are not to be executed. Credit institutions and financial institutions are entitled to request that the authority decide whether concerns exist about the immediate execution of a transaction; if the authority (Article 6 Security Police Act) fails to make respond by the end of the ensuing banking day, then the transaction may be executed immediately. Credit institutions and financial institutions must pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing, in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose. Credit institutions and financial institutions must keep suitable records on such activities.

(1a) Credit institutions must immediately inform the authority (para. 1) of all requests to withdraw savings deposits if

1. the requests are submitted after 30 June 2002, and
2. the customer's identity has not been ascertained pursuant to Article 40 para. 1 for the savings deposit and
3. the payment is from a savings deposit which shows a balance of at least EUR 15,000 or an equivalent value. Such savings deposits may not be paid out until seven calendar days after the date of the request unless the authority (para. 1) orders a longer period pursuant to para. 3.

(2) Upon request, credit institutions and financial institutions must provide the authority (para. 1) with all information which the authority deems necessary in order to prevent or pursue cases of money laundering or terrorist financing.

(3) The authority (para. 1) is empowered to order that an ongoing or upcoming transaction with respect to which there is suspicion or reason to suspect that the transaction serves the purpose of money laundering (Article 165 StGB – including asset components which stem directly from a criminal act on the part of the perpetrator) or terrorist financing (Article 278d StGB) be omitted or delayed temporarily and that customer instructions

involving outgoing funds only be executed with the consent of the authority. The authority must inform the customer and the public prosecutor's office of this instruction without unnecessary delay. The notification to the customer must include an indication that the customer or another party concerned is entitled to lodge a complaint with the Independent Administrative Tribunal regarding violations of his/her rights; in this context, the notification must also refer to the provisions regarding such complaints contained in Article 67c of the General Law on Administrative Procedure (*Allgemeines Verwaltungsverfahrensgesetz – AVG*).

(3a) The authority must reverse the instruction pursuant to para. 3 as soon as the conditions for its issue are no longer fulfilled or the public prosecutor declares that the conditions for confiscation pursuant to Article 109 no. 2 and Article 115 para. 1 no. 3 Criminal Procedure Code are not fulfilled. Otherwise, the instruction is to be abrogated

1. once six months have elapsed since it was issued;
2. as soon as the court has issued a legally effective decision on a request for confiscation pursuant to Article 109 no. 2 and Article 115 para. 1 no. 3 Criminal Procedure Code.

(3b) Vis-à-vis customers and third parties, credit institutions and financial institutions must maintain the confidentiality of all operations which serve the purpose of compliance with paras. 1 to 3. As soon as an instruction pursuant to para. 3 has been issued, however, credit institutions and financial institutions are empowered to refer the customer to the authority (Article 6 Security Police Act); with the consent of the authority, those institutions are also empowered to inform the customer of the instruction themselves. The prohibition pursuant to this paragraph

1. does not refer to disclosures to the FMA or the Oesterreichische Nationalbank, or to disclosures for law enforcement purposes;
2. is not to prevent disclosures between institutions from Member States, or from third countries provided that they fulfil the requirements set forth in Article 40a para. 1, belonging to the same group as defined in Article 2 (12) of Directive 2002/87/EC;
3. is not, in cases related to the same customer and the same transaction involving two or more institutions, to prevent disclosures between the relevant institutions provided that they are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in Directive 2005/60/EC, and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged is to be used exclusively for the purposes of the prevention of money laundering and terrorist financing.

The FMA must inform the competent authorities of the other Member States and the European Commission of cases where the FMA considers that a third country fulfils the conditions set forth in no. 1 or 2. If the European Commission adopts a decision pursuant to Article 40 (4) of Directive 2005/60/EC, the Austrian federal government must, in agreement with the Main Committee of the National Council, issue a regulation prohibiting disclosures between credit/financial institutions and institutions/persons from the third country in question.

(4) Credit institutions and financial institutions must

1. establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.
2. communicate the relevant policies and procedures to their branches and subsidiaries in third countries;

3. take suitable measures to familiarise the staff responsible for the execution of transactions with the provisions intended to prevent or suppress money laundering or terrorist financing; these measures must also include the participation of the responsible employees in special training programmes in order to train the employees to recognise transactions which may be connected to money laundering or terrorist financing and to behave correctly in such cases;
4. establish systems which enable them to respond fully and rapidly to enquiries from the authority (Article 6 Security Police Act) or from the FMA as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship where those authorities consider such enquiries necessary in order to prevent or pursue cases of money laundering or terrorist financing;
5. allow the FMA to review the effectiveness of systems for the suppression of money laundering or terrorist financing at any time;
6. nominate within the undertaking a special officer to ensure compliance with Articles 40 et seq. for the suppression of money laundering and terrorist financing.

The authority (Article 6 Security Police Act) must provide credit institutions and financial institutions with access to up-to-date information on the practices of money launderers and terrorist financiers and on indications leading to the recognition of suspicious transactions. Likewise, the authority must ensure that, wherever practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided.

(5) Should the FMA or the Oesterreichische Nationalbank, in performing their duties of banking supervision, find reason to suspect that a transaction serves the purpose of money laundering or terrorist financing, they must report this to the relevant authority (para. 1) without delay.

(6) The following must not be used to the detriment of the accused or suspected accessories, otherwise they shall be rendered null and void:

1. data collected by the authority pursuant to para. 1, 2 or 5 in proceedings carried out exclusively due to fiscal offences, with the exception of the fiscal offences of smuggling or evasion of import or export duties, which are subject to the competence of the courts;
2. data collected by the authority pursuant to para. 1a in proceedings carried out exclusively due to fiscal offences pursuant to no. 1 or due to another criminal act punishable with no more than one year of imprisonment.

If the authority (para. 1) finds reason only to suspect a criminal act pursuant to no. 1 or 2, then it must refrain from reporting the act in accordance with Article 78 Criminal Procedure Code or Article 81 Fiscal Penalties Act (*Finanzstrafgesetz – FinStrG*).

(7) Damage claims may not be asserted due to the fact that a credit institution or financial institution or one of its employees has delayed or omitted the execution of a transaction in negligent ignorance of the fact that the suspicion of money laundering or terrorist financing or of violations pursuant to Article 40 para. 2 was incorrect.

(8) *removed (Federal Law Gazette I No. 108/2007)*

## **BWG Banking Act**

### **VII. Savings Deposits**

#### **Savings Documents**

**Article 31.** (1) Savings deposits refer to funds which are deposited with credit institutions and are not intended for payment transactions, but for investment, and as such can only be accepted against the delivery of certain documents (savings documents). Savings documents can be issued with a certain designation, in particular in the name of the customer identified pursuant to Article 40 para. 1; the use of names other than that of the customer identified pursuant to Article 40 para. 1 is not permitted under any circumstances.

(2) Savings documents may only be issued by credit institutions which are authorised to conduct savings deposit business. The designations Sparbuch (savings passbook), Sparbrief (savings certificate) or any other combination of words containing the fragment spar (savings) may be used only for these documents. The designation Sparkassenbuch (savings bank passbook) is reserved exclusively for the savings documents issued by credit institutions which are full members of the Austrian Association of Savings Banks (Fachverband der Sparkassen). The issuance of savings documents with a designation containing the elements spar (savings) or Sparkasse (savings bank) in combination with the word Post (post office / postal) is reserved exclusively for the Austrian Postal Savings Bank (Österreichische Postsparkasse).

(3) Savings deposits which amount to less than EUR 15,000 or an equivalent value and which are not registered in the name of the customer identified pursuant to Article 40 para. 1 must be subject to the restriction that the customer may only access the savings deposit upon provision of a password defined by the customer. This restriction must be recorded in the savings document and in the credit institution's records. Where the restriction is subject to the provision of a password, the party presenting the savings document must indicate the password when accessing the savings deposit. If this party is not able to do so, then he/she must present evidence of his/her right of disposal over the savings deposit. Article 40 para. 1 no. 4 is to remain unaffected by this provision. Savings deposits acquired by way of succession upon the death of a customer may be accessed without the provision of the password; the same applies to cases where a savings document is presented in the course of judicial or administrative enforcement proceedings.

(4) A credit institution which receives a report on the loss of a savings document along with an indication of the name, address and birth date of the party incurring the loss must enter the alleged loss in the records for the savings deposit in question and must not pay out any funds from the savings deposit within four weeks of receiving such a report.

(5) After 30 June 2002, savings documents for which the customer's identity has not been ascertained pursuant to Article 40 para. 1 must not be transferred or acquired in legal transactions.

#### **Deposits, Withdrawals and Interest**

**Article 32.** (1) Every deposit credited to a savings deposit and every withdrawal from a savings deposit must be recorded in the savings document.

(2) Withdrawals from a savings deposit may only be made upon presentation of the savings document itself. Deposits into a savings deposit may also be accepted in cases where the savings document is not presented simultaneously. Such deposits are to be recorded in the savings document upon the next presentation of the savings document.

(3) Savings deposits must not be accessed by means of funds transfers, except in cases where the person entitled to the savings deposit is deceased, is a minor or otherwise under tutelage, and the competent court for probate, guardianship or tutelage matters orders such a transfer, nor by means of cheques. In contrast, funds transfers to a savings deposit are permissible.

(4) Notwithstanding a restriction on the right of disposal pursuant to Article 31 para. 3 and notwithstanding Article 40 para. 1 no. 4, the credit institution is entitled to pay out funds against presentation of the savings document and subject to the requirements indicated under nos. 1 to 3 as follows:

1. In the case of savings deposits which amount to less than EUR 15,000 or an equivalent value and which are not registered in the name of a customer identified pursuant to Article 40 para. 1, withdrawals may be paid out upon provision of the password;
2. In the case of savings deposits which amount to at least EUR 15,000 or an equivalent value or which are registered in the name of the customer identified pursuant to Article 40 para. 1, withdrawals may only be paid out to the customer identified pursuant to Article 40 para. 1;
3. In the case of savings deposits which are not registered in the name of the customer identified pursuant to Article 40 para. 1 and whose balance has reached or exceeded EUR 15,000 or an equivalent value since the last presentation of the savings document exclusively as a result of interest credits, withdrawals may be paid out upon provision of the password at the first presentation of the savings document after the limit is reached or exceeded; in this context, the limit is considered to be reached or exceeded exclusively due to interest credits in cases where no credits from funds transfers have been recorded since the last presentation of the savings document which, in total, cause the above-mentioned limit to be reached or exceeded.

Withdrawals may be made subject to the provisions indicated above unless the savings document has been reported lost, withdrawal has been officially prohibited or the accounts have been frozen.

(5) Unless a savings deposit is paid out in full within a calendar year, savings deposits must be balanced at the end of each calendar year (closing date). This does not apply to savings certificates.

(6) The annual interest rate applicable to a savings deposit and any fees charged for services in connection with savings deposits must be indicated in a conspicuous place in the savings document. Each change in the annual interest rate must be recorded in the savings document upon the next presentation of the savings document along with an indication of the date on which the interest rate takes effect. The amended annual interest rate applies from the date on which it goes into effect without requiring cancellation by the credit institution.

(7) Interest on deposits into savings deposits is to begin accruing as of the value date (Article 37), with a month counted as 30 days and a year counted as 360 days. Amounts which are withdrawn within 14 days after being deposited are not to accrue interest; in this context, withdrawals from savings deposits must always be debited against the amounts most recently deposited. In the case of withdrawals from savings deposits, the interest on the amount withdrawn must be calculated up to and including the calendar day preceding the date of the withdrawal.

(8) Savings deposits may be committed for a certain term. Payments made prior to the end of the term are to be treated as advances, and interest is to be calculated accordingly. For these advances, 0.1% is to be charged for each full month by which the commitment period is not observed. However, interest on advances must not exceed the total credit interest accrued on the amount accepted; to the extent necessary, charges may be applied retroactively to credit interest paid out in the preceding year in cases where the credit interest for the current year is not sufficient. After 30 June 2002, term commitments may only be agreed upon in cases where the customer's identity has been ascertained pursuant to Article 40 para. 1.

(9) The general provisions of the statute of limitations apply to limitations on claims arising from savings deposits. Interest on savings deposits is subject to the same limitations as deposits. Limitation periods are interrupted by every interest credit recorded in the savings document and by every deposit or withdrawal.

## BWG Banking Act

### IX. Banking Secrecy

**Article 38.** (1) Credit institutions, their members, members of their governing bodies, their employees as well as any other persons acting on behalf of credit institutions must not divulge or exploit secrets which are revealed or made accessible to them exclusively on the basis of business relations with customers, or on the basis of Article 75 para. 3 (banking secrecy). If the functionaries of authorities as well as the Oesterreichische Nationalbank acquire knowledge subject to banking secrecy requirements in the course of performing their duties, then they must maintain banking secrecy as official secrecy; these functionaries may only be relieved of this obligation in the cases indicated under para. 2. The obligation to maintain secrecy applies for an indefinite period of time.

(2) The obligation to maintain banking secrecy does not apply

1. vis-à-vis public prosecutors and criminal courts in connection with criminal court proceedings on the basis of a court approval (Article 116 Criminal Procedure Code; *Strafprozeßordnung – StPO*), and vis-à-vis the fiscal authorities in connection with initiated criminal proceedings due to wilful fiscal offences, except in the case of financial misdemeanours;
2. in the case of obligations to provide information pursuant to Article 41 paras. 1 and 2, Article 61 para. 1, Article 93 and Article 93a;
3. vis-à-vis the probate court and the court commissioner in the event of the death of a customer;
4. vis-à-vis the competent court for guardianship or tutelage matters if the customer is a minor or otherwise under tutelage;
5. if the customer grants his/her express written consent to the disclosure of secrets;
6. for general information commonly provided in the banking business on the economic situation of an undertaking, unless the undertaking expressly objects to the provision of such information;
7. where disclosure is necessary in order to resolve legal matters arising from the relationship between the credit institution and customer;
8. with regard to the reporting requirements pursuant to Article 25 para. 1 of the Inheritance and Gift Tax Act (*Erbschafts- und Schenkungssteuergesetz*);
9. in the case of obligations to provide information to the FMA pursuant to the Securities Supervision Act and the Stock Exchange Act.

(3) A credit institution may not invoke its banking secrecy obligations in cases where the disclosure of secrets is necessary in order to determine the credit institution's own tax liabilities.

(4) The provisions of paras. 1 to 3 also apply to financial institutions and contract insurance undertakings with regard to Article 75 para. 3 and to protection schemes, with the exception of cooperation with other protection schemes, deposit guarantee schemes and investor compensation schemes as required by Articles 93 to 93b.

(5) (**constitutional law provision**) Paras. 1 to 4 may only be amended by the National Council with at least one-half of the representatives present and with a two-thirds majority of the votes cast.

**BWG Banking Act****XXII. Procedural and Penal Provisions**

**Article 70.** (1) In its area of responsibility as the banking supervisory authority (Article 69 para. 1 nos. 1 and 2), the FMA may, notwithstanding the powers conferred on the basis of other provisions of this federal act, do the following at any time for the purpose of supervising credit institutions and groups of credit institutions:

1. demand that credit institutions and superordinate credit institutions on behalf of undertakings in the group of credit institutions present interim financial statements, reports in specified forms and using specified layouts, and audit reports; require credit institutions and superordinate credit institutions on behalf of undertakings in the group of credit institutions as well as their governing bodies to provide information on all business matters; inspect bookkeeping records, documents and data media; Article 60 para. 3 is applicable to the scope of the FMA's information, presentation and inspection rights as well as the obligation to make documents available in Austria;
  2. obtain audit reports and information from the bank auditors of credit institutions and groups of credit institutions as well as the competent auditing associations; in addition, the FMA may obtain all necessary information from, and provide all necessary information to, the protection schemes and the government commissioner appointed pursuant to para. 2 no. 2;
  - 2a. have the bank auditors of credit institutions and groups of credit institutions, other external auditors and external auditing companies, the competent auditing associations and other experts conduct all necessary audits; the reasons for exclusion indicated in Article 62 are applicable in this context; the FMA is permitted to provide information to the auditors it engages where this serves the purpose of fulfilling the audit engagement;
  3. instruct the Oesterreichische Nationalbank to conduct audits of credit institutions, their branches and representative offices outside of Austria, of credit institutions which are subject to supplementary supervision pursuant to Article 5 para. 1 Financial Conglomerates Act and of undertakings within the group of credit institutions. The competence of the Oesterreichische Nationalbank to conduct on-site inspections in the field of Banking Supervision and in credit institutions or groups of credit institutions in financial conglomerates applies to inspections of all lines of business and all risk types. The Oesterreichische Nationalbank must ensure that it has sufficient personnel and organisational resources at its disposal to conduct the audits indicated. The FMA is authorised to have its own employees participate in audits conducted by the Oesterreichische Nationalbank;
  4. also request that the competent authorities in the host Member State conduct audits of undertakings in a group of credit institutions and of branches and representative offices in Member States and in third countries pursuant to Article 77 para. 5 nos. 2 and 3 where this simplifies or expedites the process compared to an audit pursuant to no. 3 or where this is in the interest of expedience, simplicity, speed or cost-effectiveness; under these circumstances, the Oesterreichische Nationalbank may also be obliged to participate in such audits, and FMA employees may participate in such audits.
- (1a) Where the Oesterreichische Nationalbank determines in the course of an on-site inspection that the audit engagement issued in accordance with para. 1 no. 3 or 4 is not sufficient to attain the objective of the audit, the Oesterreichische Nationalbank must request the necessary extensions from the FMA. The FMA must either extend the audit engagement or reject the extension with an indication of the reasons for the rejection without delay, at the latest, however, within one week.
- (1b) The FMA and the Oesterreichische Nationalbank must jointly define an audit plan for each upcoming calendar year. The audit plan must take the following into account:

1. audits of system-relevant credit institutions;
2. an appropriate frequency of audits of non-system-relevant institutions;

3. resources for ad-hoc audits;
4. thematic focuses of audits;
5. the review of measures taken to remedy the defects identified.

The audit plan must define the focuses of audits and audit start dates for each specific institution. Where the Oesterreichische Nationalbank determines that an on-site inspection is necessary in order to fulfil the criteria pursuant to nos. 1 to 5 and such an on-site inspection is not defined in the joint audit plan, the Oesterreichische Nationalbank is authorised and obliged to request that the FMA issue an additional audit engagement. This request must include a proposal for the content of the audit engagement and indicate the reasons justifying an unscheduled inspection for the purposes of nos. 1 to 5. The FMA must either issue the audit engagement or reject the request with an indication of the reasons for the rejection without delay, at the latest, however, within one week. The FMA's right to issue audit engagements pursuant to para. 1 nos. 3 and 4 is to remain unaffected by this provision.

(1c) The Oesterreichische Nationalbank is authorised to carry out on-site inspections pursuant to para. 1 no. 3 for macroeconomic reasons without an audit engagement from the FMA if the audits defined in the audit plan pursuant to para. 1b or other FMA audit engagements are not affected. The Oesterreichische Nationalbank must inform the FMA of such inspections and indicate the reasons for the inspections by the time they begin.

(1d) The Oesterreichische Nationalbank must define the intended scope of the inspection pursuant to para. 1c in writing. The examiners must deliver a copy of this document to the credit institution upon starting the inspection. In cases where the credit institution audited refuses to grant access or to cooperate as necessary for the purpose of carrying out the inspection, the FMA must ensure that the scope of the inspection as defined in writing is enforced in accordance with Article 22 Financial Market Authority Act at the Oesterreichische Nationalbank's request.

(2) In cases of danger to the fulfilment of the credit institution's obligations to its creditors, in particular to the security of assets entrusted to the credit institution, the FMA may issue an administrative ruling (*Bescheid*) ordering measures for a limited period of time in order to avert that danger; such measures must be abrogated at the latest 18 months after going into effect. In particular, the FMA may issue administrative rulings (*Bescheide*) which

1. completely or partly prohibit withdrawals of capital and earnings as well as distributions of capital and earnings;
2. appoint an expert supervisor (government commissioner) who is an attorney at law or external auditor; in the case of credit cooperatives, it is also possible to appoint auditors from cooperative auditing associations; the supervisor, who has all of the rights pursuant to para. 1 nos. 1 and 2, must
  - a) prohibit the credit institution from any transactions which might serve to exacerbate the danger mentioned above, and/or
  - b) in cases where the credit institution is completely or partly prohibited from continuing business/transactions, allow individual transactions which do not exacerbate the danger mentioned above;
3. completely or partly prohibit directors of the credit institution from managing the credit institution, with simultaneous notification of the body responsible for appointing the directors; the responsible body must re-appoint the corresponding number of directors within one month; in order to be legally effective, such appointments require the consent of the FMA, which must refuse to grant consent if the newly appointed directors do not appear suitable for the purpose of averting the danger mentioned above;
4. completely or partly prohibit the continuation of business operations.

(2a) At the request of the supervisor appointed pursuant to para. 2 no. 2 or para. 3 (government commissioner), the FMA may appoint a deputy if and as long as this is necessary for important reasons, especially in cases where the supervisor is temporarily prevented from performing his/her duties. The provisions applicable to the supervisor also apply to the appointment of the supervisor as well as his/her rights and duties. Given the approval of the FMA, the supervisor (government commissioner) may employ persons with suitable professional qualifications where necessary in light of the scope and difficulty of the duties to be performed. The FMA's approval must name these persons specifically and must also be delivered to the relevant credit institution. These persons are to act upon the instructions of and on behalf of the supervisor (government commissioner) or his/her deputy.

(2b) The procedure pursuant to para. 2 is a reorganisation measure as defined in Article 2 of Directive 2001/24/EC. Articles 81 to 81m are applicable; in this context, the receivership procedure is considered a procedure pursuant to para. 2, and the FMA must issue a decree of appointment to the government commissioner. Article 83 paras. 4 to 9 are applicable; in this context, the receivership procedure is considered a procedure pursuant to para. 2, and the FMA is to act in lieu of the court.

(3) The FMA must obtain reports on suitable government commissioners from the Austrian Bar Association (*Österreichischer Rechtsanwaltskammertag*), from the Chamber of Professional Accountants and Tax Advisors (*Kammer der Wirtschaftstreuhänder*), from the cooperative auditing associations. Where a government commissioner pursuant to para. 2 no. 2 or a deputy pursuant to para. 2a is to be appointed and such an appointment not possible on the basis of those reports, the FMA must notify the Bar Association or chamber of professional accountants and tax advisors which is responsible for the credit institution's place of incorporation or the relevant cooperative auditing association so that the relevant organisation may name an attorney or external auditor with suitable professional qualifications for the position of government commissioner. In cases of imminent danger, the FMA may appoint (1) an attorney or (2) an external auditor as a temporary government commissioner. This appointment will be abrogated once an attorney or external auditor has been appointed in accordance with the first sentence.

(4) In cases where a licensing requirement pursuant to Article 5 *para. 1 nos. 1 to 14* or pursuant to Article 5 para. 4 after the licence is issued, or where a credit institution violates the provisions of this federal act, the Savings Bank Act, the Building Society Act, the Regulation Implementing the Mortgage Bank Act and Mortgage Bond Act, the Mortgage Bank Act, the Mortgage Bond Act, the Act on Funded Bank Bonds, the Investment Fund Act, the Depository Act, the Participation Fund Act, the E-Money Act, the Act on Severance and Retirement Funds for Salaried Employees and Self-Employed Persons, the Real Estate Investment Fund Act, the Financial Conglomerates Act, regulations issued on the basis of these federal acts, or an administrative ruling (*Bescheid*), the FMA must

1. instruct the credit institution on pain of penalties to restore legal compliance within a period of time which is appropriate in light of the circumstances;
2. in cases of repeated or continued violations, completely or partly prohibit the directors from managing the credit institution, unless this would be inappropriate based on the nature and severity of the violation and the restoration of legal compliance can be expected through repetition of the procedure pursuant to no. 1; in such cases, the initial penalty imposed must be enforced and the instruction repeated on pain of a higher penalty;
3. revoke the licence in cases where other measures pursuant to this federal act cannot ensure the functioning of the credit institution.

(4a) Where a violation of this federal act leads to the inadequate limitation of the risks arising from the banking transactions and banking operations of the credit institution or the group of credit institutions (Articles 39 and 39a) and the proper capture and limitation of risks cannot be expected in the short term, the FMA must, notwithstanding other measures in accordance with this federal act, impose a minimum capital requirement on the credit institution or group of credit institutions up to a maximum of 150% of the minimum capital requirement pursuant to Article 22 para. 1 with regard to certain exposures. The FMA must also impose

additional capital requirements in accordance with this paragraph in cases where other measures pursuant to this federal act, especially an instruction pursuant to para. 4 no. 1, are not sufficient to ensure the proper capture and limitation of risks as well as compliance with legal regulations. In cases where the FMA first proceeds in accordance with para. 4 no. 1, it may impose additional capital requirements in accordance with this paragraph immediately if the instruction is unsuccessful.

(5) Any and all measures ordered by the FMA pursuant to paras. 2 and 2a are to be suspended for the duration of a receivership procedure (Section XVII).

(6) The government commissioner is to be remunerated by the FMA with a fee (function fee) which is commensurate to the work involved in supervision and the expenses incurred for this purpose. The government commissioner is entitled to submit invoices for each previous quarter and after the termination of his/her activities. The FMA must effect remuneration immediately after reviewing the invoice.

(7) The FMA is entitled to inform the public of measures taken by the FMA pursuant to paras. 2, 3 and 4 by placing an announcement in the Official Gazette of the *Wiener Zeitung*, in a newspaper distributed throughout Austria, on the Internet, or by posting a bulletin at a suitable location on the business premises of the credit institution. However, measures pursuant to para. 4 no. 1 are only to be published where this is necessary for the purpose of informing the public in light of the nature and severity of the violation. These publication measures may be taken in full or in part.

(8) Credit institutions must inform the chairperson of the supervisory body immediately of all administrative rulings (*Bescheide*) issued by the FMA on the basis of the provisions set forth in Article 69.

(9) The FMA must convey administrative rulings (*Bescheide*) with which directors are completely or partly prohibited from managing the credit institution (para. 2 no. 3 and para. 4 no. 2) as well as any reversals of such measures to the Commercial Register Court for entry in the Commercial Register.

(10) In the case of representative offices of credit institutions incorporated in a Member State or in a third country, the FMA may obtain the information indicated in para. 1 nos. 1 to 3 as well as other information and have audit activities conducted in order to monitor compliance with Article 1 para. 1 and Article 73; para. 7 is applicable in this context. In cases where these provisions are violated, the FMA must, Article 98 para. 1 notwithstanding,

1. take the measures indicated in Article 15 in the case of credit institutions pursuant to Article 9;
2. take the measures indicated in Article 70 para. 4 nos. 1 and 2 in the case of credit institutions from third countries and inform the competent authority in the relevant credit institution's country of incorporation accordingly.

**Article 70a.** (1) In cases where the parent undertaking of a credit institution is a mixed-activity holding company, then the FMA is entitled, notwithstanding the powers conferred to the FMA on the basis of other provisions of this federal act, to request from the credit institution all information necessary for the purpose of supervision on the mixed-activity holding company as the parent undertaking and on its subsidiary undertakings at any time for the sake of ongoing supervision of credit institutions. Those undertakings must make all documents available to the credit institution and provide all information necessary in order for the credit institution to fulfil its obligation to provide information to the FMA.

(2) Notwithstanding the powers existing on the basis of other provisions in this federal act, the FMA may, in accordance with Article 70 para. 1 no. 3, instruct the Oesterreichische Nationalbank to obtain all information to be provided by the credit institution pursuant to para. 1 on site and to review the information provided; Article 70 para. 1 no. 3 (third sentence) and Article 71 are applicable in this context. It is also possible to instruct the bank auditors, the competent auditing associations, external auditors or other experts independent of the mixed-activity holding company to conduct the audit.

(3) *removed*

(4) In cases where the mixed-activity holding company or one of its subsidiary undertakings is incorporated in another Member State, the FMA must request that the competent authorities in the other Member State conduct the audit pursuant to para. 2.

(5) In cases where the parent undertaking of a credit institution is a mixed-activity holding company, then the FMA is entitled, notwithstanding the powers conferred to the FMA on the basis of other provisions of this federal act, to supervise the transactions between the credit institution, the mixed-activity holding company and its subsidiary undertakings. For this purpose, the credit institution must have in place adequate risk management processes and internal control mechanisms, including sound reporting and accounting procedures, so that the credit institution's transactions with the parent undertaking and its subsidiaries can be identified, measured, monitored and controlled appropriately. In this context, the credit institution must – beyond reports to the Major Loans Register pursuant to Article 75 – report material intra-group transactions, especially loans, guarantees, off-balance-sheet transactions, cost-sharing agreements, reinsurance transactions, capital investment transactions and transactions concerning own funds, to the FMA on at least a quarterly basis. Where these intra-group transactions pose a threat to a credit institution's financial position, the FMA will take appropriate measures.

.../...

**Article 96.** In the enforcement of administrative rulings (*Bescheide*) pursuant to this federal act, the amount of EUR 30,000 is to replace the amount of ATS 10,000 provided for in Article 5 para. 3 Act on Administrative Enforcement (*Verwaltungsvollstreckungsgesetz – VVG*). The enforcement of such administrative rulings by way of monetary fines as coercive penalties is also permissible against public authorities.

**Article 97.** (1) The FMA must charge credit institutions the following rates of interest on the following amounts:

1. 2% on the amount by which the credit institution falls below the capital requirement pursuant to Article 22 para. 1 in conjunction with Article 103, calculated on an annual basis, for 30 days, except in the case of supervisory measures pursuant to Article 70 para. 2 or in cases where the credit institution is over indebted;
2. 5% over the applicable bank rate on the amount by which the credit institutions falls below Liquidity 1 funds pursuant to Article 25 para. 7, calculated on an annual basis, for 30 days; the amounts by which the credit institution falls short of its minimum reserve requirement (Article 5 of Regulation (EC) No. 2818/98 of the European Central Bank of 1 December 1998 on the application of minimum reserves, OJ L 356 of 30 December 1998) are to be deducted from the Liquidity 1 shortfall;
3. 2% on the amount by which the credit institutions falls below Liquidity 2 funds pursuant to Article 25 para. 12, calculated on an annual basis, for 30 days;
4. *removed*; This English translation of the authentic German text serves merely information purposes. The official wording in German can be found in the Austrian Federal Law Gazette (*Bundesgesetzblatt – BGBl.*). 177
5. 0.5% on the amount by which the credit institution exceeds the limits on open term positions pursuant to Article 26a paras. 2 and 3, calculated on an annual basis, for 30 days, except in the case of supervisory measures pursuant to Article 70 para. 2 or in cases where the credit institution is over indebted;
6. 2% on the amount by which the credit institution exceeds large exposure limits pursuant to Article 27 para. 7 in conjunction with Article 103, calculated on an annual basis, for 30 days, except in the case of supervisory measures pursuant to Article 70 para. 2 or in cases where the credit institution is overindebted;
7. *removed*.

(2) The interest amounts required pursuant to para. 1 are to be paid to the federal government.

**Article 98.** (1) Parties who conduct banking transactions without the required authorisation are guilty of an administrative offence and are to be punished by the FMA with a fine of up to EUR 50,000 unless the act constitutes a criminal offence falling into the jurisdiction of the courts.

(2) Parties who, as persons responsible (Article 9 Act on Administrative Penalty [*Verwaltungsstrafgesetz – VStG*]) for a credit institution,

1. fail to notify the FMA in writing in accordance with Article 10 para. 5 regarding changes in the information pursuant to Article 10 para. 2 nos. 2 to 4 and para. 4 no. 2;
2. fail to notify the FMA regarding the activities indicated in Numbers 1 to 14 of Annex I to Directive 2006/48/EC in accordance with Article 10 para. 6;
3. fail to notify the FMA in writing of any acquisition and any disposal pursuant to Article 20 paras. 2 and 4 in accordance with Article 20 para. 5;
4. fail to notify the FMA in writing in accordance with Article 20 para. 5 of the identity of shareholders and other members holding qualifying participations as well as the amounts of such participations as shown in particular in the information received for the annual general meeting of shareholders or other members, or in the information received on the basis of Articles 91 to 94 Stock Exchange Act.
- 4a. fail to notify the FMA in writing of the result of the election of the chairman of the supervisory board pursuant to Article 28a para. 4;
5. fail to provide the superordinate credit institution with all information required for consolidation in accordance with Article 30 para. 7;
6. violate the obligations set forth in Articles 40, 40a, 40b, 40d and 41 paras. 1 to 4;
7. fail to notify the FMA immediately in writing of the circumstances indicated in Article 73 para. 1 nos. 1 to 15;
8. fail to submit the reports specified in Article 74 to the FMA or the Oesterreichische Nationalbank within the defined periods and in accordance with the form requirements set forth by law or regulation, or repeatedly submit inaccurate or incomplete reports;
9. fail to comply with the duty to report major loans pursuant to Article 75;
10. advertise their membership in a deposit guarantee or investor compensation scheme in an impermissible manner (Article 93 para. 11);
11. violate the notification obligations set forth in Articles 21a para. 3 nos. 1 and 2, 21c para. 3 nos. 1 and 2, 21d para. 3 nos. 1 and 2, 21e para. 4 nos. 1 and 2, 21f para. 7 nos. 1 and 2, 22o para. 4, 22q para. 3 as well as 73 paras. 4 and 4a, or the presentation and reporting requirements set forth in Article 44 paras. 1 to 6;

are guilty of an administrative offence and are to be punished by the FMA with a fine of up to EUR 30,000 unless the act constitutes a criminal offence falling into the jurisdiction of the courts.

(3) Parties who, as persons responsible (Article 9 Act on Administrative Penalty) for a credit institution,

1. fail to indicate the annual interest rate applicable to a savings deposit in a conspicuous place in the savings document in accordance with Article 32 para. 6;
2. fail to record changes in the annual interest rate in the savings document upon the next presentation of the document, including an indication of the date on which the interest rate takes effect;
3. fail to comply with the written form requirement when concluding consumer credit agreements (Article 33 para. 2) and consumer current account agreements (Article 34 para. 2);

4. conclude consumer credit agreements which do not contain the information required pursuant to Article 33 para. 2 nos. 1 to 5;
5. conclude consumer credit agreements for revolving credit facilities which do not contain the information required pursuant to Article 33 para. 3;
6. fail to announce changes in the effective and/or notional annual interest rate in writing before it takes effect;
7. fail to provide an annual account statement pursuant to Article 33 para. 9;
8. conclude consumer current account agreements which do not contain the information required pursuant to Article 34 para. 2;
9. fail to inform the customer of his/her account balance on a quarterly basis in accordance with Article 34 para. 4;
10. fail to post the information required pursuant to Article 35 para. 1 and Article 103 no. 32 in the lobby or fail to provide depositors with required information;
11. advertise the willingness to extend credit as specified in Article 35 para. 2 without indicating the effective and/or notional annual interest rate;
- 11a. fail to comply with the price display requirement pursuant to Article 35 para. 3 in its entirety;
12. violate the due diligence obligations pursuant to Article 36,

are guilty of an administrative offence and are to be punished by the FMA with a fine of up to EUR 3,000 unless the act constitutes a criminal offence falling into the jurisdiction of the courts.

(4) Parties who, as the persons responsible (Article 9 Act on Administrative Penalty) for a credit institution, violate the regulation prohibiting disposals over accounts pursuant to Article 78 para. 7, even through mere negligence, are guilty of an administrative offence and are to be punished by the FMA with a term of imprisonment of up to six weeks and a fine of up to EUR 50,000 unless the act constitutes a criminal offence falling into the jurisdiction of the courts.

**Article 99.** Parties who

1. as the persons responsible (Article 9 Act on Administrative Penalty) for a financial institution, fail to provide the FMA with the information pursuant to Article 12 para. 3 or fail to notify the FMA in accordance with Article 12 para. 5;
2. as the persons responsible (Article 9 Act on Administrative Penalty) for a financial institution, fail to provide the FMA with the information pursuant to Article 14 para. 3 or fail to notify the FMA in accordance with Article 14 para. 5;
3. intend to hold a qualifying participation in a credit institution directly or indirectly and fail to notify the FMA accordingly in advance and in writing, including an indication of the amount of the participation, pursuant to Article 20 para. 1.
4. intend to increase a qualifying participation in a credit institution in such a way that the limits of 20%, 33% or 50% of the voting rights or capital are reached or exceeded, or in such a way that the credit institution becomes a subsidiary undertaking of that party, and fail to notify the FMA accordingly in advance and in writing pursuant to Article 20 para. 2;
5. intend to dispose of a qualifying participation in a credit institution or to fall below the limits for participations in credit institutions as indicated in Article 20 para. 2 and fail to notify the FMA accordingly in advance and in writing pursuant to Article 20 para. 4;

6. as the persons responsible (Article 9 Act on Administrative Penalty) for a subordinate institution or a superordinate financial holding company, fail to provide the superordinate credit institution with all of the information required for consolidation in accordance with Article 30 para.
- 7; 6a as the persons responsible (Article 9 Act on Administrative Penalty) for a mixed-activity undertaking or its subsidiary, fail to provide the credit institution with all of the information required pursuant to Article 70a para. 1; 7. use the designation "*Sparbuch*" (savings passbook), "*Sparbrief*" (savings certificate) or "*Sparkassenbuch*" (savings bank passbook) without authorisation in violation of Article 31 para. 2;
8. as the persons responsible (Article 9 Act on Administrative Penalty) for a financial institution, violate the obligations set forth in Articles 40, 40a, 40b, 40d and 41 paras. 1 to 4;
9. fail to comply with their disclosure obligations as trustees pursuant to Article 40 para. 2 or Article 103 no. 24;
10. as bank auditors, violate Article 63 para. 3 by failing to notify the FMA and the Oesterreichische Nationalbank in writing of facts or justified doubts identified by the bank auditors pursuant to Article 63 para. 3 along with explanations immediately, or in the case of slight defects which can be remedied in the short term only once the bank fails to remedy the defects within a period of no more than three months as stipulated by the bank auditor, or fail to submit notification when the directors fail to provide information requested by the bank auditor within the period defined by the bank auditor; this also applies to the persons named in accordance with Article 88 para. 7 Professional Code of Conduct for Certified Public Accountants and Tax Advisors in cases where an external auditing company is appointed as the bank auditor;
11. as the persons responsible (Article 9 Act on Administrative Penalty) for a representative office, fail to comply with the reporting requirements set forth in Article 73 para. 2 within one month;
12. as the persons responsible (Article 9 Act on Administrative Penalty) for a financial institution or a contract insurance undertaking, fail to comply with the obligation to report major loans pursuant to Article 75;
13. as the persons responsible (Article 9 Act on Administrative Penalty) for a protection scheme, fail to submit the annual financial statements of the protection scheme to the FMA pursuant to Article 93a para. 8 within six months of the end of the business year;
14. as the persons responsible (Article 9 Act on Administrative Penalty) for a protection scheme, fail to report the withdrawal of a credit institution from the protection scheme to the FMA pursuant to Article 93a para. 8;
15. use the designation "*Geldinstitut*" (money institution), "*Kreditinstitut*" (credit institution), "*Finanzinstitut*" (financial institution), "*Finanz-Holdinggesellschaft*" (financial holding company), "*Wertpapierfirma*" (investment firm), "*Kreditunternehmung*", "*Kreditunternehmen*" (credit undertaking), "*Bank*" (bank), "*Bankier*" (banker), "*Sparkasse*" (savings bank), "*Bausparkasse*" (building society), "*Volksbank*" (people's bank), "*Landes-Hypothekenbank*" (state mortgage bank), "*Raiffeisen*" or any designation containing one of those words without authorisation in violation of Article 94;
16. as the persons responsible (Article 9 Act on Administrative Penalty) for a credit institution or as the auditor pursuant to Article 230a General Civil Code, violate the provisions governing cover reserves pursuant to Article 230a General Civil Code (Articles 66 to 68);
17. execute disposals over accounts or provides other financial services in violation of directly applicable provisions of EU law, without such disposals constituting an administrative offence pursuant to the Foreign Exchange Act;
18. contractually transfer or acquire savings documents for which the customer's identity has not been ascertained pursuant to Article 40 para. 1 in violation of Article 31 para. 5;

19. fail to collect, store, review or forward the necessary information, or carry out or accept funds transfers in violation of Articles 5 to 14 of Regulation (EC) No. 1781/2006 on information on the payer accompanying transfers of funds, or violate record-keeping or notification obligations,

are guilty of an administrative offence and are to be punished by the FMA with a fine of up to EUR 30,000, in the case of no. 10 up to EUR 50,000, unless the act constitutes a criminal offence falling into the jurisdiction of the courts.

**Article 99a.** (1) If, as the superordinate institution, a financial holding company fails to provide the superordinate credit institution with all of the information required for consolidation pursuant to Article 30 paras. 7 and 8 despite measures pursuant to Article 99 no. 6 in conjunction with Article 96, and if this objective cannot be attained through other measures, then the FMA may request the suspension of voting rights for the shares held by group institutions in these subordinate institutions from the competent first-instance commercial courts at the domestic subordinate institutions' place of incorporation.

(2) If a court orders the suspension of voting rights in accordance with para. 1, then the court must simultaneously appoint and transfer the exercise of the voting rights to a trustee who fulfils the requirements of Article 5 para. 1 no. 3. The voting rights of the shareholders are to be suspended until the court has established that the conditions pursuant to para. 1 are no longer fulfilled. This must be communicated to the FMA.

(3) The trustee has the right to reimbursement of his/her expenses and to remuneration for his/her activities in an amount to be determined by the court. The financial holding company and the subordinate institution concerned are to bear joint and several liability for those expenses and remuneration. The obliged parties may appeal decisions determining the amount of remuneration for the trustee and the expenses to be reimbursed to him/her. Appeals beyond rulings of the provincial superior court will not be permitted.

**Article 99b.** In the case of administrative offences pursuant to Articles 98 and 99, a limitation period of 18 months applies instead of the limitation period of six months set forth in Article 31 para. 2 of the Act on Administrative Penalty.

**Article 100.** (1) Parties who conduct banking transactions without the required authorisation are not entitled to any remuneration, especially interest and commissions, associated with those transactions. The legal invalidity of agreements associated with those transactions does not render the overall banking transaction legally invalid. Agreements to the contrary as well as suretyships and guarantees associated with those transactions are legally invalid.

(2) Parties who conduct banking transactions without the required authorisation cannot invoke Article 1 para. 5.

**Article 101.** (1) Parties who disclose or exploit facts subject to banking secrecy in order to create an economic advantage for themselves or others, or in order to place others at a disadvantage, are to be punished by the court with a term of imprisonment of up to one year or with a fine of up to 360 day-fines.

(2) In the case of para. 1, the offender is to be prosecuted only with the authorisation of the person whose interest in secrecy was violated.

**VAG Insurance Supervision Act**

**Eighth Chapter**

**PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

**Scope of application and definitions**

**Article 98a.** (1) The provisions of the present Chapter shall apply to insurance undertakings within the scope of the operation of the life assurance business.

(2) For the purposes of the present Chapter, the following definitions shall apply:

1. “Politically exposed persons” are understood to be persons exercising prominent public functions or having exercised them up until a year ago, their immediate family members or persons known to be close associates of such persons.

a) In this context, “prominent public functions” shall include the following:

aa) heads of state, heads of government, ministers, deputy ministers and state secretaries;

bb) members of parliaments;

cc) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

dd) members of courts of auditors or of the boards of central banks;

ee) ambassadors, chargés d’affaires and high-ranking officers in the armed forces;

ff) members of the administrative, management or supervisory bodies of state-owned enterprises.

The categories set out in sublit. aa to ee shall include positions at Community and international level.

b) “Immediate family members” shall include the following:

aa) the spouse;

bb) any partner considered by national law as equivalent to the spouse;

cc) the children and their spouses or partners considered by national law as equivalent to the spouse;

dd) the parents.

c) “Persons known to be close associates” shall include the following:

aa) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, such as foundations or trusts, with a person entrusted with a prominent public function, or any other close business relations with a person entrusted with a prominent public function;

bb) any natural person who has sole beneficial ownership of a legal entity or legal arrangement, such as foundations or trusts, which is known to have been set up for the benefit de facto of the person entrusted with a prominent public function.

2. “Business relationship” shall mean a business relationship between the insurance undertaking and the customer(s), entered into upon conclusion of an insurance contract, the assumption of an insurance contract or the assignment of a claim arising from an insurance contract.

3. “Beneficial owner” shall mean the natural persons who ultimately own or control the customer. The term of “beneficial owner” shall include in particular:

a) in the case of corporate entities:

aa) the natural persons who ultimately own or control a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25% plus one share shall be deemed sufficient to meet this criterion;

bb) the natural persons who otherwise exercise control over the management of a legal entity;

b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

aa) where the future beneficiaries have already been determined, the natural persons who are the beneficiaries of 25% or more of the allocations of a trust or legal entity;

bb) where the individuals that benefit from the trust or legal entity have yet to be determined, the class of persons in whose main interest the trust or legal entity is set up or operates;

cc) the natural persons who exercise control over 25% or more of the property of a trust or legal entity.

4. "Customer" shall mean the policyholder and the beneficiary from the insurance contract. Persons to whom claims arising from an insurance contract are assigned shall be deemed equivalent to the beneficiary.

#### **Due diligence obligations for combating money laundering and terrorist financing**

**Article 98b.** (1) Insurance undertakings shall identify and verify the identity of a customer:

1. prior to establishing a business relationship;

2. prior to carrying out any transactions that are not within the scope of a business relationship and that amount to at least EUR 15,000 or their euro equivalent, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked; if the amount is not known at the beginning of the transaction, their identity shall be established as soon as the amount becomes known and has been determined as amounting to at least EUR 15,000 or their euro equivalent;

3. if there is suspicion or reasonable grounds to suspect that the customer belongs to a terrorist organisation (Article 278b StGB; Federal Law Gazette no. 60/1974) or that the customer objectively participates in transactions which serve money laundering purposes (Article 165 StGB – including asset components which stem from a criminal offence committed by the perpetrator himself) or to finance terrorism (Article 278d StGB);

4. when there are doubts about the authenticity or adequacy of previously obtained customer identification data.

The identity of a customer shall be established by personal presentation of an official photo identification document. Any documents issued by a government authority shall be deemed an official photo identification document if they come with a non-replaceable photo of the head of the person concerned, and if they include the name, the date of birth and the signature of the person as well as the authority issuing the document. In the case of travel documents of foreigners, the full date of birth need not be included in the travel document if this complies with the law of the state issuing the document. In the case of legal persons and natural persons without legal capacity, the identity of the natural person holding the power of representation shall be established by presentation of his official photo identification document and the power of representation verified by means of appropriate certificates. The identity of a legal person shall be established by means of meaningful supporting documents which are available pursuant to the legal standards prevailing in the country of the head office of the legal person. Only in the cases pursuant to paras. 98c and 98e shall deviations from the aforementioned provisions be allowed. Not all of the criteria applicable to the official photo identification document will have to

be met if, due to reasons of technological progress, other equivalent criteria such as biometric data are introduced which are at least equivalent to the criteria repealed with respect to proving identity. However, the criterion that the document must have been issued by a government authority shall always be met.

(2) The insurance undertaking shall request the person planning to establish a business relationship with the insurance undertaking to inform it about whether he acts as trustee; the request must be met. If he announces that he will act as trustee, he shall also furnish proof of the trustor's identity to the insurance undertaking. The trustee shall be identified pursuant to para. 1, exclusively with his physical presence. Identifying the trustee by third parties shall also be ruled out. In the case of natural persons, the identity of the trustor shall be established by presentation of the original or a copy of the trustor's official photo identification document (para. 1); in the case of legal persons, by means of meaningful supporting documents pursuant to para. 1. Furthermore, the trustee shall make a written statement to the insurance undertaking stating that he personally or by way of reliable sources convinced himself of the identity of the trustor. Courts and other government authorities, notaries public, lawyers and third parties as defined by Article 98e shall be deemed reliable sources within this meaning.

(3) Moreover, insurance undertakings shall undertake to:

1. ask the customer to make known the identity of the customer's beneficial owner, which he must comply with, and take risk-based and adequate measures to verify his identity so that they are satisfied that they know who the beneficial owner is, including, as regards legal persons or trusts, take risk-based and adequate measures to understand the ownership and control structure of the customer;
2. take risk-based and adequate measures to obtain information on the purpose and intended nature of the business relationship;
3. take risk-based and adequate measures to conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the insurance undertaking's knowledge of the customer, the business and risk profile, including, where necessary, the source of monies or financial funds and ensure that the documents, data or information held are kept up-to-date.

(4) Insurance undertakings shall subject their transactions to a risk analysis on the basis of appropriate criteria (products, customers, complexity of transactions, business of customers, geography in particular) concerning the risk of being misused for the purpose of money laundering or for the purpose of terrorist financing. Insurance undertakings must furnish proof to the FMA that the extent of the measures taken as a result of the analysis can be deemed appropriate with respect to the risks of money laundering and terrorist financing.

(5) By way of derogation from para. 1 no. 1, insurance undertakings may also allow the verification of the identity of the beneficiary under the insurance contract to take place only before the time of payout or when the beneficiary exercises his rights vested under the insurance contract.

(6) In the event that the insurance undertaking is unable to comply with paras. 1 to 3 pertaining to customer identification and obtaining other necessary information about the business relationship, they may not establish a business relationship or carry out any transactions; moreover, the sending of a report about the customer to the authority (Article 6 of the *Sicherheitspolizeigesetz* [SPG; Security Police Act], Federal Law Gazette no. 566/1991) pursuant to Article 98f para. 1 should be considered.

(7) Insurance undertakings shall apply the customer due diligence procedures on customer identification and verification procedures in accordance with the present Chapter not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis.

(8) Insurance undertakings shall undertake to:

1. arrange that measures are applied in their branches and subsidiaries located in third countries which are at least equivalent to those laid down in this federal act with regard to customer due diligence and record keeping;

2. inform the FMA where the legislation of the third country does not permit application of the measures required under no. 1 and to take additional measures to effectively handle the risk of money laundering or terrorist financing.

The FMA shall inform the competent authorities of the other signatory countries and the European Commission of cases where the legislation of the third country does not permit application of the measures required under no. 1 and coordinated action could be taken to pursue a solution.

(9) In connection with non-cooperative countries, Article 78 para. 9 BWG, Federal Law Gazette no. 532/1965, shall be applied correspondingly.

### **Simplified customer due diligence**

**Article 98c.** (1) Insurance undertakings shall be relieved of the obligations required under Article 98b para. 1 nos. 1, 2 and 4, paras. 2 and 3 in the following cases, subject to assessment of whether situations represent a low risk of money laundering or terrorist financing pursuant to para. 2:

1. where the customer is:

- a) an insurance undertaking, provided it is subject to the provisions of the present Chapter, a credit institution pursuant to Article 1 para. 1 BWG or a credit or financial institution pursuant to Article 3 of Directive 2005/60/EC (Official Journal L 309 of 25 November 2005, p. 15);
- b) an insurance undertaking, a credit or financial institution situated in a third country within the meaning of Article 3 of Directive 2005/60/EC which imposes requirements equivalent to those laid down in Directive 2005/60/EC and is supervised for compliance with those requirements;
- c) listed companies whose securities are admitted to trading on a regulated market in one or several signatory countries and listed companies from third countries which are subject to disclosure requirements consistent and comparable with Community legislation, in accordance with a regulation to be issued by the FMA on the basis of its authority to issue regulations pursuant to Article 85 para. 10 BörseG;
- d) a domestic public authority; or
- e) a public authority or public institution:
  - aa) provided it has been entrusted with public responsibilities on the basis of the Treaty on European Union, the EC Treaty or the European Union's secondary law;
  - bb) whose identity is publicly verifiable and transparent and has been established without doubt;
  - cc) whose activities and accounting policies are transparent; and
  - dd) if it is accountable to a body of the European Union or the authorities of a signatory country, or there are other control and counter-control mechanisms to examine its activities.

2. vis-à-vis customers in respect of the following insurance contracts and related transactions:

- a) life assurance contracts where the annual premium is no more than EUR 1,000 or the single premium is no more than EUR 2,500;
- b) insurance contracts for pension schemes if there is no surrender clause and they cannot be used as collateral for a loan.

(2) Insurance undertakings shall assess whether there is little risk of money laundering or terrorist financing with the customers referred to in para. 1 no. 1 lit. c to e and the products referred to in para. 1 no. 2 lit. b. In this context, special attention shall be paid to the activities of said customers and the kind of products and transactions from which an increased probability can be inferred that they are used for money laundering or terrorist financing purposes. When it can be inferred from the information available to insurance undertakings

that the risk of money laundering or terrorist financing might not be low, the exemptions laid down in this paragraph shall not apply.

(3) Insurance undertakings shall keep appropriate records in order to be able to prove that the conditions for applying simplified customer due diligence procedures are met.

(4) The federal government shall order - in agreement with the Main Committee of the National Council - that exemptions pursuant to para. 1 are not to be applied if the European Commission adopts a decision pursuant to Article 40(4) of Directive 2005/60/EC.

(5) The FMA shall inform the competent authorities of other signatory countries and the European Commission of cases in which, in its opinion, a third country meets the conditions as set forth in para. 1.

#### **Enhanced customer due diligence**

**Article 98d.** (1) Insurance undertakings shall apply, on a risk-sensitive basis, enhanced customer due diligence measures, in addition to the obligations referred to in Article 98b paras. 1 to 3 and 7, in situations which by their nature can present a higher risk of money laundering or terrorist financing. At any rate, they shall additionally:

1. where the customer or the natural person holding his power of representation pursuant to Article 98b para. 1 has not been physically present for identification purposes, and the personal presentation of an official photo identification document was therefore not possible, take specific and adequate measures to compensate for the higher risk; they shall ensure – other than in the event of suspicion or reasonable grounds to suspect in accordance with Article 98b para. 1 no. 3, as no business relationship must be established in these cases at any rate – that at least:

either

a) the contractual declaration of the customer is available either by means of a qualified electronic signature pursuant to Article 2 no. 3a of the *Signaturgesetz* (SigG; Signature Act), Federal Law Gazette I no. 190/1999; or, if this is not the case, the contractual declaration of the insurance undertaking is made in writing and sent by registered post to that customer address which has been given as the customer's residence or head office;

b) they know the name, date of birth and address of the customer, in the case of legal persons, the company name and the head office; in the case of legal persons, the head office must also be the seat of the central administration, about which the customer shall be required to make a written statement. Moreover, a copy of the official photo identification document of the customer or his legal representative or, in the case of legal persons, of the body holding the power of representation must be submitted to the insurance undertaking prior to the establishment of the business relationship, unless the legal transaction is effected electronically by virtue of a qualified electronic signature;

c) if the head office or residence is situated outside the EEA, that there is a written confirmation by a credit institution with which the customer has established a permanent business relationship, which states that the customer has been identified within the meaning of Article 98b paras. 1, 2, para. 3 nos. 1 or 2 and/or Article 8(1)(a) to (c) of Directive 2005/60/EC and that the permanent business relationship is being maintained. If the head office of the credit institution issuing the confirmation is situated in a third country, said third country shall set standards that are equivalent to the standards set by Articles 16 to 18 of the aforementioned Directive. In lieu of an identification and confirmation by a credit institution, an identification and written confirmation by the Austrian representation in the third country concerned or a recognised certification agency shall also be admissible;

or

d) the first payment within the scope of the business relationship is carried out through an account opened in the customer's name with a credit institution pursuant to Article 98e para. 1 no. 3 and para. 2; in this case, name, date of birth and address of the customer, in the case of legal persons, the

company name and the head office must be known and copies of the customer's documents must be available, based on which the details of the customer or the natural person holding his power of representation can be convincingly verified. Instead of said copies it suffices if there is a written confirmation by the credit institution through which the first payment is carried out which states that the customer has been identified within the meaning of Article 98b paras. 1, 2, para. 3 nos. 1 or 2 and/or Article 8(1)(a) to (c) of Directive 2005/60/EC.

No. 1 shall not apply, subject to assessment of whether situations represent a low risk of money laundering and terrorist financing, with respect to the insurance contracts and related transactions mentioned under Article 98b para. 1 no. 2.

2. in respect of transactions or business relationships with politically exposed persons of other signatory countries or third countries:

- a) have appropriate risk-based procedures to determine whether the customer is a politically exposed person;
- b) obtain senior management approval for establishing business relationships with such customers;
- c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction; and
- d) conduct enhanced ongoing monitoring of the business relationship.

(2) Insurance undertakings shall scrutinise with special care every establishment of a business relationship and each transaction that in their opinion makes it particularly likely that the business relationship or transaction may be connected with money laundering (Article 165 StGB – including asset components which stem from a criminal offence committed by the perpetrator himself) or terrorist financing (Article 278d StGB) and, if necessary, take measures to forestall that they are being used for money laundering or terrorist financing purposes.

#### **Performance by third parties**

**Article 98e.** (1) Insurance undertakings may rely on third parties to meet the obligations laid down in Article 98b paras. 1, 2 and 3 nos. 1 and 2. However, the ultimate responsibility for meeting those obligations shall remain with the insurance undertaking which relies on the third party. For the purposes of this paragraph, “third parties” shall mean:

1. insurance undertakings subject to the provisions as laid down in the present Chapter, insurance undertakings as defined in Article (3)(2)(b) of Directive 2005/60/EC;
2. insurance intermediaries pursuant to Article 365 para. 3 no. 4 GewO 1994, insurance intermediaries as defined in Article 3(2)(e) of Directive 2002/92/EC;
3. credit institutions pursuant to Article 1 para. 1 BWG, credit and financial institutions as defined in Article 3(1) and (2)(a)(c)(d) and (f) of Directive 2005/60/EC; unless they are authorised to exclusively carry out the operations of a currency exchange office (bureaux de change) (Article 1 para. 1 no. 22 BWG) or a money transmission or remittance office (Article 1 para. 1 no. 23 BWG);
4. the persons referred to in Article 2(1)(3)(a) and (b) of Directive 2005/60/EC whose head offices are situated within the domestic territory or the EEA.

(2) Legal or natural persons situated in a third country which are equivalent to those referred to in para. 1 shall be deemed third parties within the meaning of para. 1 on condition that they:

1. are subject to mandatory professional registration, recognised by law; and
2. apply customer due diligence requirements and record keeping requirements as laid down in the present Chapter or equivalent to those laid down in Directive 2005/60/EC and their compliance with the

requirements of this Directive is supervised in accordance with Section 2 of Chapter V, or they are situated in a third country which imposes equivalent requirements to those laid down in this Directive.

The FMA shall inform the competent authorities of other signatory countries and the European Commission of cases in which, in its opinion, a third country meets the aforementioned conditions.

(3) Where the European Commission adopts a decision pursuant to Article 40(4) of Directive 2005/60/EC, the federal government shall - in agreement with the Main Committee of the National Council - prohibit insurance undertakings by regulation from relying on third parties from the third country concerned to meet the obligations laid down in Article 98b paras. 1, 2 and 3 nos. 1 and 2.

(4) Insurance undertakings shall arrange that third parties make information requested in accordance with the obligations laid down in Article 98b paras. 1, 2 and 3 nos. 1 and 2 and/or in Article 8(1)(a) to (c) immediately available to them. Furthermore, insurance undertakings shall arrange that relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner are immediately forwarded, on their request.

(5) This paragraph shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the insurance undertaking which is obliged to meet the obligations laid down in Article 98b paras. 1, 2 and 3 nos. 1 and 2.

### **Reporting obligations**

**Article 98f. (1)** If there is suspicion or reasonable grounds to suspect:

1. that the intended establishment of a business relationship or an existing business relationship serves money laundering purposes (Article 165 StGB– including asset components which stem from a criminal offence committed by the perpetrator himself);
2. that a transaction which has already been carried out, is ongoing or imminent serves money laundering purposes (Article 165 StGB– including asset components which stem from a criminal offence committed by the perpetrator himself);
3. that the policyholder failed to comply with the obligation to disclose trusts pursuant to Article 98b para. 2;
4. that a customer belongs to a terrorist organisation pursuant to Article 278b StGB, or that the establishment of a business relationship or the transaction serves to finance terrorism pursuant to Article 278d StGB,

the insurance undertaking shall immediately notify the authority (Article 6 SPG) thereof and refrain from establishing the business relationship or carrying out any transaction until the facts have been ascertained, unless there is danger that this would complicate or hinder the investigation of the facts. Insurance undertakings shall pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing. This concerns in particular complex or unusual contract terms and transactions which have no apparent economic or visible lawful purpose. Suitable records thereof shall be kept. Insurance undertakings shall be entitled to demand a decision from the authority (Article 6 SPG) whether there are objections to the immediate carrying out of a transaction; if the authority (Article 6 SPG) does not reply by the end of the following bank working day, the transaction may be carried out without delay.

(2) Insurance undertakings shall provide any information to the authority (Article 6 SPG), at its request, which it deems necessary to prevent or prosecute money laundering or terrorist financing.

(3) The authority (Article 6 SPG) shall be authorised to direct that an ongoing or imminent transaction with respect to which there is suspicion or reasonable grounds to suspect that it serves money laundering purposes (Article 165 StGB – including asset components which stem from a criminal offence committed by the perpetrator himself) or to finance terrorism (Article 278d StGB) is not carried out or preliminarily postponed. The authority (Article 6 SPG) shall inform the public prosecutor's office of the directive without unnecessary

delay. The notification of the customer shall include a note that he or another individual concerned are entitled to file an appeal against violation of their rights to the *Unabhängiger Verwaltungssenat* (UVS; Independent Administrative Tribunal); it must also include a note on the provisions contained in Article 67c of the *Allgemeines Verwaltungsverfahrensgesetz* (AVG; Code of Administrative Procedure) 1991, Federal Law Gazette no. 51/1991.

(4) The authority (Article 6 SPG) shall revoke the directive pursuant to para. 3 as soon as the conditions for issuing it cease to exist or the state prosecutor's office declares that the conditions for a seizure pursuant to Article 109 no. 2 and Article 115 para. 1 no. 3 StPO 1975, Federal Law Gazette no. 631/1975, do not exist. Moreover, the directive shall expire:

1. if six months have passed since it was issued; or
2. as soon as the court has finally decided on an application for seizure pursuant to Article 109 no. 2 and Article 115 para. 1 no. 3 StPO.

(5) Insurance undertakings shall treat as confidential any and all events which serve compliance with paras. 1 to 3 vis-à-vis customers and third parties. As soon as a directive pursuant to para. 3 has been issued, they shall be authorised to refer the customer to the authority (Article 6 SPG); with the consent of the authority (Article 6 SPG), they shall also be authorised to inform the customer of the directive themselves. The prohibition laid down in this paragraph:

1. shall not refer to the disclosure of information to the FMA, the Oesterreichische Nationalbank or the disclosure of information for the purposes of prosecution;
2. shall not prevent disclosure between subsidiaries from signatory countries, or from third countries provided that they meet requirements equivalent to those laid down in Directive 2005/60/EC, belonging to the same group as defined by Article 2(12) of Directive 2002/87/EC and are supervised for compliance with those requirements;
3. in cases related to the same customer and the same transaction involving two or more insurance undertakings pursuant to Article 98e para. 1 no.1 or credit institutions pursuant to Article 98e para. 1 no. 3, this shall not prevent disclosure between them provided that they are situated in a signatory country, or in a third country which imposes requirements equivalent to those laid down in Directive 2005/60/EC, and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged shall be used exclusively for the purposes of the prevention of money laundering and terrorist financing.

The FMA shall inform the competent authorities in the other signatory countries and the European Commission of cases in which, in their opinion, a third country meets the conditions as set forth in nos. 2 and 3. Where the European Commission adopts a decision pursuant to Article 40(4) of Directive 2005/60/EC, the federal government shall - in agreement with the Main Committee of the National Council - prohibit by regulation disclosure amongst insurance undertakings and persons from the third country concerned.

(6) If the FMA has reasons to suspect, when exercising insurance supervision, that a business relationship or transaction serves money laundering or terrorist financing purposes, it shall inform the authority (Article 6 SPG) thereof without delay.

(7) Data which was investigated by the authority (Article 6 SPG) pursuant to paras. 1, 2 or 6 must not be used, otherwise becoming null and void, to the detriment of the accused or intervening third parties in proceedings conducted exclusively in respect of financial offences, with the exception of financial offences falling under the jurisdiction of the courts, of smuggling or the evasion of import or export duties. If the authority (Article 6 SPG) merely suspects a criminal offence in accordance with the first sentence, it shall not make a report pursuant to Article 78 StPO or Article 81 of the *Finanzstrafgesetz* (FinStrG; Tax Offences Act), Federal Law Gazette no. 129/1958.

(8) No claims for damages may be asserted owing to the fact that an insurance undertaking or one of its employees carried out a transaction late or not at all as a result of a negligent lack of knowledge that the suspicion of money laundering or terrorist financing or the suspicion of violation as defined in Article 98b para. 2 was false.

#### **Record keeping and statistical data**

**Article 98g.** Insurance undertakings shall keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the authority (Article SPG) or the FMA:

1. any and all documents which serve as identification pursuant to Article 98b paras. 1 to 3 and 7 as well as supporting evidence and records on the insurance contract for at least five years following the termination of the insurance contract;
2. the supporting evidence and records for a period of at least five years following the carrying out of the transactions.

#### **Internal procedures and training**

**Article 98h.** (1) Insurance undertakings shall undertake to:

1. establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent business relationships and transactions related to money laundering or terrorist financing;
2. communicate relevant policies and procedures to its branches and subsidiaries in third countries;
3. take appropriate measures so that their employees entrusted with the establishment of business relationships and the carrying out of transactions are aware of the provisions in force to prevent or combat money laundering or terrorist financing. These measures shall include, among other things, participation of the relevant employees in special ongoing training programmes to help them recognise the conclusion of contracts or transactions which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases;
4. have systems in place that enable them to respond fully and rapidly to enquiries from the authority (Article 6 SPG) or the FMA, which they deem necessary to prevent or prosecute money laundering or terrorist financing, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship;
5. enable the FMA to review the effectiveness of their systems to combat money laundering or terrorist financing;
6. provide for a special person charged with guaranteeing compliance with Articles 98a to 98h to combat money laundering and terrorist financing.

(2) The authority (Article 6 SPG) shall ensure that insurance undertakings have access to up-to-date information on the practices of money launderers and terrorist financiers and on indications leading to the recognition of suspicious business relationships and transactions. It shall also ensure that, wherever practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided.

## **Financial Market Authority Act (FMABG)**

### **Liability for the FMA's Activities**

**Section 3** (1) The Federal Government shall be liable pursuant to the provisions of the *Amtshaftungsgesetz* (AHG; Public Liability Act), Federal Law Gazette no. 20/1949, for damage caused by the FMA's bodies and employees in the enforcement of the federal acts specified under section 2. The FMA as well as its employees and bodies shall not be liable towards the injured party.

(2) In its activities, the FMA shall take any and all supervisory measures that are necessary, expedient and appropriate in each case after a due assessment of the circumstances. To this end, it shall take care to maintain financial market stability. In the performance of its duties, it may use the audit reports of the statutory auditors and bodies of the companies subject to its supervision as well as the audit reports of the Oesterreichische Nationalbank (OeNB) within the scope of its statutory auditing powers pursuant to the BWG, unless it has reasonable doubts about the correctness or completeness of said audit reports or about the professional know-how or diligence of the auditors or should have had such doubts if it had shown adequate diligence. The same shall apply to the audit reports of the auditors commissioned by the FMA itself with regard to the auditing activities pursuant to the federal acts specified under section 2.

(3) If the Federal Government made good the damage to the injured party pursuant to section 1, it shall be entitled to demand reimbursement from the FMA's bodies or employees according to the provisions of the AHG.

(4) The FMA shall support the Federal Government in public liability and reimbursement proceedings pursuant to paras 1 and 2 in any appropriate way. In particular, it shall provide any information and documents which concern the public liability and reimbursement proceedings and ensure that the Federal Government can make use of the know-how and knowledge of the FMA's bodies and employees about the supervisory measures pertaining to the proceedings.

(5) The statutory auditors appointed by the companies subject to supervision shall not be deemed bodies within the meaning of section 1 para 1 AHG, unless they perform audits pursuant to the federal acts specified under section 2 for the FMA upon its separate order. The same shall apply to the auditing bodies of legally competent auditing institutions.

**GewO Trade Act**  
**General provisions**

**1. Scope**

**Article 1** (1) This Federal Act shall apply, unless otherwise provided by Articles 2 to 4, to all trade or business activities that are not prohibited by law.

(2) An activity shall be deemed to be of a trade or business nature if it is performed on a self-employed basis, regularly and with the aim of reaping profits or other economic benefits, irrespective of the latter's intended purpose; no difference shall be made between whether the intended profits or other economic benefits are to be reaped in the context of an activity falling within the scope of this Federal Act, or whether they are to be reaped in the context of an activity not falling within the scope of this Federal Act.

(3) Self-employment as defined by this Federal Act refers to an activity performed for one's own account and at one's own risk.

(4) Also any one-time activity is deemed to be of a regular nature if its circumstances imply any intention of repeating such activity, or if it requires a longer period of time. Offering any activity of a trade or business nature to a larger group of people or within tenders shall be deemed to be equivalent to carrying on a trade or business.

(5) The intention of reaping profits or other economic benefits shall also be regarded as such when such profits or other economic benefits are intended for the members of a partnership.

(6) In the case of associations as defined by the Associations Act 1951 (Vereinsgesetz 1951– VerG 1951) the intention of reaping profits or other economic benefits shall also be regarded as such when the activity of the association gives the impression of that of a trade or business undertaking, and when this activity – be it directly or be it indirectly – is aimed at reaping financial benefits for the members of such an association. Whenever an association performs an activity under the VerG 1951 more than once a week which, if done for trade or business purposes, would fall within the scope of this Federal Act, it shall be presumed that there is the intention of reaping profits or other economic benefits.

...

**Article 13** (1) Natural persons shall be excluded from carrying on any trade or business if they

1. have been sentenced by any court

a) for fraudulently withholding payment of social insurance contributions and surcharges under the Construction Workers' Leave and Severance Pay Act (Bauarbeiter-Urlaubs- und Abfertigungsgesetz – BUAG) – art. 153d of Criminal Code (Strafgesetzbuch – StGB) –, for organised undeclared work – art. 153e StGB –, fraudulent bankruptcy, damage to creditors, preference of any creditor, or grossly negligent injury to any creditors' interests (art. 156 to 159 StGB), or

b) for any other criminal offence to a term of imprisonment of more than three months or a fine of more than 180 daily rates, and

2. the sentence has not yet been removed from the criminal record.

Natural persons shall be excluded from carrying on any restaurant or catering business if their record includes a court sentence for infringement of art. 28 to 31a of the Narcotic Drugs Act (Suchtmittelgesetz, SMG), Federal Law Gazette I no. 112/1997, as amended. Concerning fines that are not based on daily rates, the alternative sentence of imprisonment (for failure to pay the fine) shall be relevant. If both a term of imprisonment and a fine have been imposed, the former and the alternative sentence shall be added up. For this purpose one month shall be equivalent to thirty days. The provisions of this paragraph shall also apply if offences comparable to those underlying the above grounds for exclusion have been committed abroad.

(2) Whoever has been sentenced by any fiscal prosecution authority for having committed fiscal offences such as smuggling, evasion of import or export taxes, handling of smuggled goods under art. 37(1)a of the Fiscal Penalties Act (Finanzstrafgesetz – FinStrG), Federal Law Gazette no. 129/1958, as amended, for non-declaration of monopoly revenues, wilful interference with any government monopoly or concealment of monopoly under art. 46(1)a of the FinStrG, shall be excluded from carrying on any trade or business if he has been sentenced to a fine of more than €726, or to both a fine and a term of imprisonment, for having committed such a fiscal offence, and if no more than five years have elapsed since sentencing. The same shall apply if offences comparable to those underlying the above grounds for exclusion have been committed abroad.

(3) Legal entities shall be excluded from carrying on any trade or business (art. 38 (2))

1. if, for presumed lack of sufficient assets to cover the cost of bankruptcy proceedings, such proceedings have not been instituted or have been discontinued, and
2. if the period of access to the insolvency case referred to above in the insolvency database has not yet elapsed.

The same shall apply if situations comparable to those underlying the above ground for exclusion have occurred abroad.

(4) Legal entities shall also be excluded from establishing any trade or business involving activities of insurance mediation, save as set out in para. 3, if bankruptcy proceedings have been instituted to realise and distribute their assets and if the period of access to the insolvency database has not yet elapsed. The same shall apply to comparable situations abroad. There shall be no ground for exclusion if bankruptcy proceedings have resulted in compulsory composition with creditors and such composition has been met, or if within bankruptcy proceedings the court has confirmed the debtor's payment plan and this plan has been met, or if, after conclusion of debt adjustment proceedings, remission of residual debt has been granted and has not been revoked.

(5) A natural person shall be excluded from carrying on any trade or business if this person has or had substantial influence on the conduct of business operations of a legal entity other than a natural person which is or was excluded from carrying on any trade or business under para. 3. If any of the grounds for exclusion referred to in para. 4 applies to the legal entity, the natural person shall only be excluded from carrying on any trade or business involving activities of insurance mediation. The last sentence of para. 1 shall apply accordingly.

(6) After having been deprived by court sentence of the right of carrying on a trade or business, or after having suffered withdrawal of one's trade or business licence under art. 87(1)3 or 4, a natural person shall be excluded from carrying on any trade or business if the performance of such a trade or business activity could frustrate the purposes underlying deprivation by court sentence or withdrawal under art. 87(1)3 or 4. This shall also apply to any natural person who has occasioned official measures under art. 91(1) or (2) for any of the reasons of withdrawal referred to in art. 87(1)3 or 4.

(7) Legal entities other than natural persons shall be excluded from carrying on any trade or business, if any natural person who has substantial influence on the conduct of business operations of this legal entity is excluded from carrying on any trade or business under paras. 1 to 3, 5 or 6. If any of the grounds for exclusion referred to in para. 4 applies to the natural person, the legal entity in question shall only be excluded from carrying on any trade or business involving activities of insurance mediation. The last sentence of para. 1 shall apply accordingly.

.../...

#### **4. Special requirements for carrying on any trade or business**

##### **Certificate of qualification**

##### **General provisions**

**Article 16** (1) Carrying on any regulated trade or business, or any part of such trade or business, shall be subject to qualification requirements. If the applicant fails to prove his qualifications, he shall appoint a managing director (art. 39). This shall also apply to the trade of chimney sweepers (art. 94(55)). In such a case art. 9(2) shall apply provided that the new managing director is appointed within one month.

(2) Certificate of qualification is to be understood in this context as meaning evidence that the applicant has the technical as well as the commercial knowledge, skills and experience to independently perform the typical activities of the trade or business in question.

(3) Evidence of the qualification of training apprentices shall be provided by passing the examination for trainers or any of its equivalents, or by completing a course for trainers or any of its equivalents (Articles 29a, 29g and 29h of the Vocational Training Act [Berufsausbildungsgesetz – BAG]).

(4) Foreign certificates of qualification for an activity equivalent to a regulated trade or business shall be deemed equivalent to Austrian certificates of qualification for a regulated trade or business if this has been set out in international treaties or in secondary legislation declaring such equivalence and issued by the Federal Minister of Economics and Labour. If requested, the authority shall issue a letter confirming such equivalence.

### **Insurance Intermediation**

**Art. 137** (1) Insurance intermediation means introducing, proposing or carrying out other work preparatory to the conclusion of contracts of insurance, or of concluding such contracts, or of assisting in the administration and performance of such contracts, in particular in the event of a claim. These activities can be activities of an insurance agent or of an insurance broker in the sense of the Act on Insurance Contracts (Versicherungsvertragsgesetz – VersVG) and the Broker Act (Maklergesetz).

.../...

### **Authorities and procedures**

#### **1. General provisions**

##### **Single point of contact**

**Article 333** (1) Unless expressly provided otherwise, authority as defined by this Federal Act, namely authority of first instance, shall mean district administration authority.

(2) Trade or business persons (Gewerbetreibende) also have the option of electronically submitting to the competent trade authority the notification they are required to submit to their competent social insurance institution (Sozialversicherungsanstalt der gewerblichen Wirtschaft) in terms of compulsorily insured self-employed at the beginning of their compulsory insurance period and the notification they are required to submit to the competent tax office in terms of legal taxpayers upon business take-up. The competent trade authority shall forthwith communicate the notification of any compulsorily insured self-employed to the competent social insurance institution and the notification of any legal taxpayer to the competent tax office.

.../...

**Article 336** (1) By using appropriate measures to prevent any risk of administrative offences and taking the necessary measures to initiate administrative penal proceedings, the Federal Police (Bundespolizei) and the officers of agencies responsible for maintaining public security (Organe des öffentlichen Sicherheitsdienstes) shall help enforce art. 366(1)(1), (2), (3), art. 367(35), (38), (50) and (51), and art. 367a, as well as prevent infringements of shop closing hours (art. 113).

(2) The officers of agencies responsible for public security referred to in para. 1 shall undertake the same efforts to help enforce art. 367 (25), provided that this concerns requirements or instructions for music performances taking place in a restaurant, bar or similar location.

(3) Where other suitable officers are available to the competent authority for the tasks referred to in para. 1, the competent authority shall deploy them in lieu of officers of agencies responsible for public security.

**Article 336a** (1) In places having federal police offices (Bundespolizeidirektionen), these shall help the district administration authorities, in terms of authorities responsible for public security in trades or businesses listed in art. 95, with the reliability checks required under this provision. Wherever this Federal Act requires assistance by the Federal Minister of the Interior or by any second (states') level public security authority (Sicherheitsdirektion) in procedures for acquiring a trade or business licence (art. 107(5), art. 132(1), art. 141(1) and art. 148), these authorities shall also help with the necessary reliability checks.

(2) The authorities defined by para. 1, which under this Federal Act shall be obliged to check the reliability of a person in terms of public security considerations, shall be authorised to process any personal data they have collected about this person in executing Federal or State Acts, and to report to the trade authorities any data raising doubts as to the reliability of the person concerned in the cases referred to in para. 1.

**Article 338** (1) Wherever necessary for executing trade law provisions, the officers of the authorities responsible for executing these provisions, as well as the experts called in by these authorities, shall be entitled to enter and visit premises and their store rooms during working hours and to control stock on hand and to inspect business records and to secure evidence. The owner of the undertaking or his deputy shall be informed no later than upon entering the premises or store room. Wherever officers of agencies responsible for public security are requested to help execute this Federal Act under art. 336, the trade or business persons shall produce and hand over for inspection all and any official documents that are of relevance to carrying on this trade or business. If any person is suspected of having committed an administrative offence under art. 366(1)(1), (2) or (3), this person shall present his ID papers to the officers of agencies responsible for public security.

(2) Wherever necessary for executing trade law provisions, the owner of the undertaking or his deputy shall enable the officers of the authorities referred to in para. 1, as well as the experts called in by these authorities, to enter and visit the premises and store rooms, as well as comply with these officers' instructions to start or stop machinery and equipment, show their mode of operation and carry out operations; moreover, he shall give to the authorities referred to under para. 1 any necessary information, submit any necessary documents and, where required, provide access to the records of stock on hand, as well as to the records of incoming and outgoing goods.

(3) Wherever necessary for executing trade law provisions, the officers of the authorities responsible for executing these provisions, as well as the experts called in by these authorities, shall also be entitled to take samples to the extent absolutely necessary. These officers or experts shall issue a written confirmation to the owner or his deputy of such samples being taken and, if requested, they shall also hand over a control sample. If requested by the owner of the undertaking, the Federal Government shall give for the sample taken some reimbursement to be determined by the competent authority in the amount of the cost price if the latter is more than €36. No such compensation will be paid if this sample has engendered a measure under art. 69(4) or art. 360, or if a specific person has been fined, or if the sample has been ordered to be forfeited.

(4) In performing their duties under paras. 1 and 2, the officers of the authorities referred to in para. 1 shall undertake efforts to avoid any unnecessary disruption or obstruction of operations.

(5) The information obtained under the last half-sentence of para. 2 shall only be used for the purposes of enforcing trade law provisions.

(6) The provisions of the Labour Inspection Act 1993 (Arbeitsinspektionsgesetz 1993 – ArbIG), Federal Law Gazette no. 27, and the provisions of the Transport Labour Inspection Act (Verkehrsarbeitsinspektionsgesetz – VAIG), Federal Law Gazette no. 650/1994, shall not be affected by this Federal Act.

(7) The officers of the authorities responsible for enforcing trade law provisions shall be entitled to inform the competent authorities whenever, within the context of their activity, they entertain well-founded suspicions of infringements of labour law or social insurance law or tax law provisions.

(8) The Federal Ministry of Economics and Labour and the Financial Market Authority (Finanzmarktaufsichtsbehörde – FMA) shall cooperate and help each other in enforcing the provisions of insurance mediation

under this Federal Act, as well as under the Banking Act (Bankwesengesetz – BWG) and the Insurance Supervision Act (Versicherungsaufsichtsgesetz – VAG).

### **r) Measures to prevent money laundering and terrorist financing**

#### **General**

**Article 365m** (1) Articles 365m to 365z transpose Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as well as Directive 2006/70/EC laying down implementing measures for Directive 2005/60/EC, for the scope of this Federal Act.

(2) The Federal Minister of Economics and Labour shall be authorised to issue secondary legislation to define the rules necessary for transposing any other implementing measures of the European Commission, especially within the meaning of art. 40 of Directive 2005/60/EC.

(3) The provisions of Articles 365m to 365z shall apply to the following trade or business persons, meaning natural persons as well as legal entities and registered partnerships:

1. dealers including auctioneers, only to the extent that payments are made in cash in an amount of €15000 or more, no matter whether the transaction is executed in a single operation or in several operations which are linked or appear to be linked;
2. real estate agents;
3. management consultants including organisation development experts when doing the following services for companies or trusts:
  - a) forming companies or other legal persons; or
  - b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; or
  - c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement; or
  - d) acting as or arranging for another person to act as a trustee of a trust or a similar legal arrangement; or
  - e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards;
4. insurance intermediaries as defined in art. 137a(1), when they act in respect of life insurance and other investment related services, unless insurance mediation is ancillary and offered only in conjunction with a main activity, and
  - a) within an individual transaction, any sales revenue from insurance mediation does not exceed 10 per cent of the sales revenue from the main transaction linked to it,
  - b) any total premium of the individual transaction, or of several transactions with a customer which appear to be linked, does not exceed €1000;
  - c) any turnover of insurance mediation does not exceed 5 per cent of the total turnover;
  - d) there is a cogent and economically useful close relationship between the mediated insurance contracts and the purpose of the trade or business person's main activity and thus the main purpose of the individual transaction, and
  - e) the main activity is not an activity under para. 3(2), (3) or (4).

(4) The financial intelligence unit (FIU) for preventing money laundering and terrorist financing shall be the Federal Minister of the Interior. The FIU shall take suspicious transaction reports under Articles 365u to 365y. The trade authority (art. 333) shall be responsible for any other administrative tasks not directly assigned to the FIU, especially the tasks to continually monitor and ensure compliance by trade and business persons with Articles 365m to 365z, including sanctioning any infringements of these provisions. The trade authority shall effectively monitor compliance with the provisions on a risk-sensitive basis and take the measures necessary to ensure such compliance. The authority shall have adequate powers and resources to perform its functions, including the power to compel the production of any information that is relevant to monitoring compliance with pertinent provisions and perform on-site inspections and checks (art. 338).

(5) Electronic money (e-money) shall be equivalent to cash.

### **Definitions**

**Article 365n** For the purposes of Articles 365m to 365z, the term:

1. "money laundering" means an offence pursuant to art. 165 of the Criminal Code (Strafgesetzbuch – StGB), Federal Law Gazette no. 60/1974 as amended
2. "terrorist financing" means the provision of a financial contribution to support a terrorist group pursuant to art. 278b StGB to commit a terrorist offence pursuant to art. 278c StGB or to complete the offence pursuant to art. 278d StGB
3. "beneficial owner" means the natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. This includes:
  - a) in the case of corporate entities:
    - aa) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25% plus one share shall be deemed sufficient to meet this criterion; or
    - ab) the natural person(s) who otherwise exercises control over the management of a legal entity; or
  - b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
    - ba) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity; or
    - bb) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; or
    - bc) the natural person(s) who exercises control over 25% or more of the property of a legal arrangement or entity.
4. "politically exposed persons"
  - a) natural persons who – with the exception of middle ranking or more junior officials – are or have been entrusted, until no more than one year ago, with one or more of the following public functions in respect of lit. aa to lit. ee, including positions at Community and international level, provided that no enhanced customer due diligence measures are to be applied on a risk-sensitive basis:
    - aa) heads of State, heads of government, ministers and deputy or assistant ministers;
    - bb) members of parliament,

- cc) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
  - dd) members of courts of auditors or of the boards of central banks;
  - ee) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
  - ff) members of the administrative, management or supervisory bodies of State-owned enterprises.
- b) family members of the persons referred to under a):
- aa) the spouse;
  - bb) any partner considered by national law as equivalent to the spouse;
  - cc) the children and their spouses or partners;
  - dd) the parents;
- c) any person known to be close associate of the persons referred to under a) who
- aa) is known to have joint beneficial ownership of legal entities or legal arrangements;
  - bb) or any other close business relationships with this person;
  - cc) has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in lit. a).

5. “business relationship” means a business, professional or commercial relationship which is connected with the professional activities of the trade or business persons covered by Articles 365m to 365t and which is expected, at the time when the contact is established, to have an element of duration.

6. “electronic money”, as defined in Article 1(3)(b) of Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, thus means a monetary value as represented by a claim on the issuer which is stored on an electronic device, issued on receipt of funds of an amount not less in value than the monetary value issued and being accepted as means of payment by undertakings other than the issuer.

### **Customer due diligence**

#### **General**

**Article 365o** The obligations set out in this section arise in the following cases:

1. when establishing a business relationship,
2. when carrying out occasional transactions amounting to €15000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
3. when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
4. when there are doubts about the veracity or adequacy of previously obtained customer identification data.

**Article 365p** (1) Customer due diligence measures shall comprise:

1. identifying the customer and verifying the customer’s identity on the basis of an official identity card with picture (amtlicher Lichtbildausweis);
2. identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that it is satisfactorily known who the beneficial owner is. As regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;

3. obtaining information on the purpose and intended nature of the business relationship; and
4. conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the entity's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

(2) The extent of customer due diligence requirements set out in para. 1 shall be determined by the actual risk profile depending on the type of customer, business relationship, product or transaction. A trade or business entity or person must be able to demonstrate the adequacy of the measures taken to the competent trade authority. Customer data shall be collected with due diligence.

(3) The obligations mentioned under para. 1 shall also be met in respect of customers already existing at the time of entry into force of these provisions.

(4) Whenever trade or business persons are unable to comply with para. 1(1) to (3), they shall be obliged to refrain from conducting transactions through a bank account, from establishing any business relationship, from carrying out the transaction, or to terminate the business relationship. More-over, they shall examine the necessity of reporting to the FIU pursuant to art. 365u(1)1.

#### **Verification of identity**

**Article 365q** (1) The verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying-out of the transaction. Real estate transactions carried out by a real estate agent shall require verification of identity if the annual rent amounts to €15000 or more. If the amount is unknown at the beginning of the transaction, the trade or business person shall verify the identity as soon as the amount is known or can be ascertained and it becomes obvious that this threshold will be reached or exceeded.

(2) By way of derogation from para. 1, verification of the identity of the customer and the beneficial owner may be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these verification procedures shall be completed as soon as practicable after the initial contact.

(3) In the case of life insurance business, verification of the identity of the beneficiary under the policy shall take place, by way of derogation from para. 1, at or before the time of payout or at or before the time the beneficiary intends to exercise rights vested under the policy.

#### **Simplified customer due diligence procedures**

**Article 365r** (1) The requirements of art. 365o(1)(1), (2) and (4), art. 365p(1) and (2) and art. 365q(1) shall not apply where the customer(s) is

1. a credit institution or financial institution covered by Directive 2005/60/EC or a credit or financial institution situated in a third country which imposes requirements equivalent to those laid down in that Directive and supervised for compliance with those requirements; or
2. listed companies whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation; or
3. domestic public authorities; or
4. public authorities or public bodies which have been entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation, whose identity is publicly available and transparent and certain, whose activities as well as their accounting

practices are transparent and are either accountable to a Community institution or the public authorities or appropriate check and balance procedures.

In these cases, trade or business persons shall gather sufficient information to establish if the customer qualifies for an exemption as mentioned in this paragraph.

(2) Furthermore, the requirements of art. 365o(1)(1), (2) and (4), art. 365p(1) and (2) and art. 365q(1) shall not apply to

1. life insurance policies where the annual premium is no more than €1000 or the single premium is no more than €2500; or
2. insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; or
3. a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; or
4. electronic money where, if the device cannot be recharged, the maximum amount stored in the electronic device is no more than €150, or where, if the device can be recharged, a limit of €2500 is imposed on the total amount transacted in a calendar year, except when an amount of €1000 or more is redeemed in that same calendar year by the bearer as referred to in art. 3 of Directive 2000/46/EC; or
5. in respect of any other savings, insurance and investment product under the following conditions:
  - a) the product has a written contractual base;
  - b) the related transactions are carried out through an account of the customer with a credit institution covered by Directive 2005/60/EC or a credit institution situated in a third country which imposes requirements equivalent to those laid down in that Directive;
  - c) the product or related transactions are not anonymous and their nature is such that it allows for the timely application of art. 365o(3);
  - d) policies where the annual premium is no more than €1000 or the single premium is no more than €2500;
  - e) the benefits of the product or related transactions cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events; and
  - f) in the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kind of contingent claims, the benefits of the product or related transactions are only realisable in the long term, the product or related transactions cannot be used as collateral and during the contractual relationship, no accelerated payments are made, no surrender clauses are used and no early termination takes place.

#### **Enhanced customer due diligence procedures**

**Article 365s** (1) Trade or business persons, in cases where the customer has not been physically pre-sent for identification purposes (distance transactions), shall send to the customer order forms at his residence or seat by means of registered mail. The customer shall be requested to add to the return-able order form a readable copy of an official identity card with picture to be used by the trade or business person to verify the data entered by the customer on his identity in the order form.

(2) In cases where the minimum estimated value, or the start price if no estimated value is indicated, and the customer's bid amount to €15000 or more, and where payment is made in cash and the customer has never been physically present for identification purposes (distance transactions), auctioneers shall request communication

of a readable copy of an official identity card with picture and use this copy to verify the customer's identity. In so doing, they shall pay special attention to offsetting the higher risk of money laundering due to the customer's physical absence by taking additional measures for data verification, such as ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

(2a) Identification within the meaning of the above two paragraphs may be dropped if the customer's identity is proved by a qualified electronic signature within the meaning of the Signature Act (Signaturgesetz), Federal Law Gazette I no. 190/1999, as amended. Art. 40b(1)(1)(b) to (d) BWG shall be applied accordingly.

(3) In respect of transactions or business relationships with politically exposed persons residing in another Member State or in a third country, trade or business persons and, where applicable, their directors and employees shall be required to:

1. have appropriate risk-based procedures to determine whether the customer is a politically exposed person;
2. have senior management approval for establishing business relationships with such customers;
3. take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction; and
4. conduct enhanced ongoing monitoring of the business relationship.

(4) Trade or business persons shall pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

### **Reporting obligations**

#### **General**

**Article 365t** Trade or business persons shall pay special attention to any transactions which they regard as particularly likely, by their nature, to be related to money laundering or terrorist financing. This applies particularly to complex or unusually large transactions or all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

**Article 365u** (1) Trade or business persons and, where applicable, their directors and employees shall:

1. promptly inform the FIU, on their own initiative, where they know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted; and
2. if requested to do so, promptly provide all the necessary information and all the necessary documents to the FIU.

(2) Information within the meaning of para. 1 shall not constitute any breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not lead to a liability of any kind.

**Article 365v** (1) Trade or business persons shall refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with art. 365u (1). The trade or business persons are entitled to ask for a decision by the FIU on whether there are any objections to forthwith carrying out the transaction. If the authority does not respond by the end of the following business day, the transaction may be carried out forthwith.

(2) Where such a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the trade or business persons concerned shall inform the FIU immediately afterwards.

(3) The FIU is authorised to order non-performance or provisional postponement of a transaction if the latter is suspected of giving rise to money laundering or terrorist financing. The FIU shall inform the customer and the public prosecutor of this order without undue delay. Information of the customer shall include a reference to the right of the customer or any other party concerned to appeal to the In-dependent Administrative Tribunal (Unabhängiger Verwaltungssenat – UVS) for infringement of their rights; this shall also include reference to the provisions governing such appeals as defined in art. 67c of the General Administrative Procedures Act (Allgemeines Verwaltungsverfahrensgesetz – AVG).

(4) The FIU shall revoke the order under para. 3 after the grounds for its issue cease to exist or the public prosecutor declares that there are no grounds for attachment. The order shall also cease to have effect when

1. six months have elapsed since its issue; or
2. the court has passed a non-appealable decision on attachment pursuant to art. 109(2) and art. 115 of the Code on Criminal Procedure (Strafprozessordnung – StPO).

**Article 365w** If, in the course of inspections carried out in trade or business persons, or in any other way, trade authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU.

#### **Prohibition of disclosure**

**Article 365x** (1) Trade or business persons and, where applicable, their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with art. 365u or that a money laundering or terrorist financing investigation is being or may be carried out.

(2) The prohibition laid down in para. 1 shall not include disclosure to the competent authorities or disclosure for law enforcement purposes.

#### **Record keeping and statistical data**

**Article 365y** (1) Trade or business persons shall keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities for at least five years after carrying out the transaction or after ending the business relationship:

1. concerning customer data a copy or the references of the evidence required including the type of document, the document number, the date of issue, the issuing authority and the country of issue; and
2. any supporting evidence and records concerning business relationships and transaction.

(2) Insurance intermediaries, when acting in respect of life insurance and other investment related services, shall apply, where applicable, also in their branches and majority-owned subsidiaries located in third countries the measures set out in the first paragraph with regard to customer due diligence and record keeping. They shall inform the FIU in writing of cases where the legislation of any third country does not permit application of such equivalent measures. The FIU shall inform the European Commission of cases where it arrives at the opinion that coordinated action could be taken to pursue a solution. Moreover, where a third country does not permit application of such measures in accordance with the first sentence, insurance intermediaries shall take additional measures to effectively handle the risk of money laundering or terrorist financing.

(3) Insurance intermediaries, when acting in respect of life insurance and other investment related services, shall have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

#### **Internal procedures, training and feedback**

**Article 365z** (1) Trade and business persons shall establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.

(2) Insurance intermediaries, when acting in respect of life insurance and other investment related services, shall also communicate, where applicable, to their branches and majority-owned subsidiaries located in third countries the measures set out in the first paragraph.

(3) Trade or business persons shall take appropriate measures so that their relevant employees are aware of the provisions in force on the prevention of money laundering and terrorist financing. These measures shall include participation of their relevant employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

(4) The Federal Minister of the Interior shall take suitable measures to inform the Federal Economic Chamber (Wirtschaftskammer Österreich – WKO) of the practices of money launderers and terrorist financiers and of indications leading to the recognition of suspicious transactions.

## **Chapter V**

### **Penal provisions**

**Article 366** (1) An administrative offence carrying a fine of up to €3600 is committed by

.../...

whoever, contrary to the provisions of art. 365u, fails to promptly inform the FIU, promptly provide all the necessary information and all the necessary documents to the FIU;

**Article 367** An administrative offence carrying a fine of up to €2180 is committed by

.../...

whoever fails to comply with the provisions of Articles 355m to 365z concerning measures to prevent money laundering and terrorist financing;

**Article 370** (1) If the appointment of a managing director has been reported or approved, any fines or other penalties shall be imposed upon this director.

(1a) Fines may also be imposed on legal persons or registered partnerships held liable for infringements referred to in Articles 365m to 365z (measures to prevent money laundering and terrorist financing) which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person or registered partnership, who has a leading position within the legal person or registered partnership, based on:

1. a power of representation of the legal person or the registered partnership;
2. an authority to take decisions on behalf of the legal person or the registered partnership, or
3. an authority to exercise control within the legal person or registered partnership.

(1b) Legal persons or registered partnerships can also be held liable for infringements referred to in Articles 365m to 365z where the lack of supervision or control by a person referred to in para. 1a has made possible the commission of the infringements referred to in para. 1a for the benefit of a legal person or registered partnership by a person under its authority.