



Cybercrime legislation – country profile

AUSTRIA

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Alexander Seger
 Department of Technical Cooperation
 Directorate General of Human Rights and Legal Affairs
 Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
 Fax: +33-3-9021-5650
 Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	AUSTRIA
Signature of Convention:	23.11.2001
Ratification/accession:	No
	<p>What measures are being undertaken in your country to become a Party?</p> <p><i>Austria intends to ratify the Convention in the course of this year. The implementation of the substantive criminal law (Article 2 to 9) of the Convention on Cybercrime was already completed with the Penal Law Amending Act 2002 (Strafrechtsänderungsgesetz 2002, Federal Law Gazette I No. 134/2002; mainly entered into force on 1st October 2002). In the range of the procedural law (Article 14 to 21) the implementation will be fully achieved with the revised Code of Criminal Procedure (Strafprozessreformgesetz, Federal Law Gazette I No. 19/2004, entered into force on 1st January 2008).</i></p>
Provisions of the Convention	Corresponding provisions/solutions in national legislation <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i>
<i>Chapter I – Use of terms</i>	
Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”	<p>Section 74 para. 1 subpara. 8 and para. 2 of the Austrian Penal Code (include the definition of “computer system” and “computer data”)</p> <p>Section 3 subpara. 2 of the Austrian E-Commerce Act (include the definition of “service provider”); the Code of Criminal Procedure refers to the definition in this Act.</p> <p>Section 92 para. 3 subpara. 4 of the Austrian Telecommunications Act 2003 (include the definition of “traffic data”)</p>
<i>Chapter II – Measures to be taken at the national level</i>	

<i>Section 1 – Substantive criminal law</i>	
Article 2 – Illegal access	Section 118a of the Austrian Penal Code
Article 3 – Illegal interception	Section 119 and 119a of the Austrian Penal Code
Article 4 – Data interference	Section 126a of the Austrian Penal Code
Article 5 – System interference	Section 126b of the Austrian Penal Code
Article 6 – Misuse of devices	Section 126c of the Austrian Penal Code
Article 7 – Computer-related forgery	Section 225a of the Austrian Penal Code
Article 8 – Computer-related fraud	Section 148a of the Austrian Penal Code
Article 9 – Offences related to child pornography	Section 207a of the Austrian Penal Code
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	Section 91 of the Federal Law on Copyright in Work of Literature and Art and on Related Rights
Article 11 – Attempt and aiding or abetting	Section 12 and 15 of the Austrian Penal Code
Article 12 – Corporate liability	Section 3 of the Federal Statute on Responsibility of Entities for Criminal Offences (<i>Verbandsverantwortlichkeitsgesetz - VbVG</i>)
Article 13 – Sanctions and measures	<u>Article 13 paragraph 1:</u> all criminal offences mentioned in Article 2 through 11 have appropriate sanctions, including also deprivation of liberty; see Section 118a, 119, 119a, 126, 126b, 126c, 148a, 225a, 207a of the Austrian Penal Code and Section 91 of the Federal Law on Copyright in Work of Literature and Art and on Related Rights; <u>Article 13 paragraph 2:</u> Section 4 of the Federal Statute on Responsibility of Entities for Criminal Offences
<i>Section 2 – Procedural law</i>	
Article 14 – Scope of procedural provisions	The common provisions, defined in Article 14 and 15, receive their attention in the Code of Criminal Procedure. It would be too extensive to mention all sections, dealing with basic procedural principles, in this questionnaire.
Article 15 – Conditions and safeguards	See comment to Article 14.
Article 16 – Expedited preservation of stored computer data	Section 109 and 134 para. 2 subpara. 2 of the revised Code of Criminal Procedure (in force from 2008-1-1); Section 103 para. 4 of the Austrian Telecommunications Act 2003
Article 17 – Expedited preservation and partial disclosure of traffic data	See comment to Article 16.
Article 18 – Production order	Section 111 para. 2, 134 para. 2 subpara. 2, 138 of the revised Code of Criminal Procedure (in force from 2008-1-1); Section 92 para. 3 subpara. 3 and 6, section 103 para. 4 of the Austrian Telecommunications Act 2003

Article 19 – Search and seizure of stored computer data	Section 109 et seq., 119 to 122 of the revised Code of Criminal Procedure (in force from 2008-1-1)
Article 20 – Real-time collection of traffic data	Section 134 and 137 of the revised Code of Criminal Procedure (in force from 2008-1-1)
Article 21 – Interception of content data	See comment to Article 20.
<i>Section 3 – Jurisdiction</i>	
Article 22 – Jurisdiction	Sections 64 and 65 of the Austrian Penal Code
<i>Chapter III – International co-operation</i>	
Article 24 – Extradition	Direct applicability of the Convention upon its ratification by Austria
Article 25 – General principles relating to mutual assistance	Direct applicability of the Convention upon its ratification by Austria; with regard to the non-extradition and subsequent prosecution of Austrian nationals see also Section 65 para. 1 subpara. 1 of the Austrian Penal Code
Article 26 – Spontaneous information	Direct applicability of the Convention upon its ratification by Austria; see also Section 55 of the Extradition and Mutual Assistance Act (ARHG), a working translation of which is attached
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	Direct applicability of the Convention upon its ratification by Austria; to be noted that under Section 3 of the ARHG, mutual assistance can be granted in the absence of a treaty on the basis of reciprocity
Article 28 – Confidentiality and limitation on use	Direct applicability of the Convention upon its ratification by Austria
Article 29 – Expedited preservation of stored computer data	Direct applicability of the Convention upon its ratification by Austria; see also Section 58 ARHG in connection with Section 143 seq. of the Austrian Code of Criminal Procedure respectively Section 115 of the revised Code of Criminal Procedure (in force from 2008-1-1)
Article 30 – Expedited disclosure of preserved traffic data	Direct applicability of the Convention upon its ratification by Austria; see also Section 58 ARHG in connection with Section 149a seq. of the Austrian Code of Criminal Procedure
Article 31 – Mutual assistance regarding accessing of stored computer data	Direct applicability of the Convention upon its ratification by Austria; see also Section 58 ARHG in connection with Section 149a seq. of the Austrian Code of Criminal Procedure
Article 32 – Trans-border access to stored computer data with consent or where publicly available	Direct applicability of the Convention upon its ratification by Austria
Article 33 – Mutual assistance in the real-time collection of traffic data	Direct applicability of the Convention upon its ratification by Austria; see also Section 58 ARHG in connection with Section 149a seq. of the Austrian Code of Criminal Procedure
Article 34 – Mutual assistance regarding the interception of content data	Direct applicability of the Convention upon its ratification by Austria; see also Section 58 ARHG in connection with Section 149a seq. of the Austrian Code of Criminal Procedure
Article 35 – 24/7 Network	Austria has already established such a point of contact. This point of contact belongs to the Federal Ministry of the Interior (Federal Office of Criminal Investigation, Department for computer and cyber crime)

	and is reachable on a twenty-four, seven-day-a-week basis.
Article 42 – Reservations	

Appendix 1: Austrian Penal Code

Treatment of all participants as offenders

Section 12. Not only the immediate offender commits the offence but also any person that instigates another person to commit it as well as everybody who is an accessory to its commission.

Punishability of attempt

Section 15. (1) The liability for intentional acts does not only apply to the completed offence but also to the attempt and to any participation in an attempt.

(2) An offence is attempted as soon as the offender materializes his decision to commit the offence or to instigate another person to do so (section 12) with an action immediately preceding the commission of the offence.

(3) The attempt and the participation in it are not punishable if the completion of the offence has been impossible under any circumstances for lack of personal features or relations requested by the law on behalf of the acting person or with respect to the act or the object against which the offence is committed.

Criminal offences abroad being punished irrespective of the laws which are valid for the scene of the crime

Section 64 (1) The Austrian penal laws are applicable regardless of the penal laws which are valid for the scene of the crime to the following offences being committed abroad:

1. espionage of a trade or business secret in favour of foreign countries (sect. 124), high treason (sect. 242), preparations for high treason (sect. 244), subversive associations (sect. 246), attacks on the high instruments of state (sects. 249 to 251), treason to the country (sects. 252 to 258) and criminal offences against the Federal Armed Forces (sects. 259 and 260);
2. criminal offences committed against an Austrian public officer (sect. 74 n.4) during or for the execution of his functions and committed by an Austrian public officer;
3. false testimony before a court (sect. 288) and perjury or false deposition under oath before an administrative authority (sect. 289) in proceedings pending in an Austrian court or in an Austrian administrative authority;
4. extortionate kidnapping (sect. 102), surrender to a foreign power (sect. 103), slave trade (sect. 104), traffic in persons (sect. 104a), transnational trafficking with prostitution (sect. 217), money counterfeiting (sect. 232), the forgery of particularly protected securities punishable under section 232 (sect. 237), criminal organization (sect. 278a para.1) and the criminal offences punishable under sects. 28 para.2 to 5, 31 para.2 and 32 para.2 of the drug law if Austrian interests have been violated or if the perpetrator cannot be extradited;
- 4a. gross sexual abuse of minors (sect. 206), sexual abuse of minors (sect. 207) and pornographic representations with minors pursuant to sect. 207a para. 1 and 2, sexual abuse of adolescent persons pursuant to sect. 207b para. 2 and 3 and promotion of prostitution and pornographic presentation of minors (sect. 215a), if the perpetrator is an Austrian citizen residing generally in the homeland;
- 4b. production and distribution of weapons for mass extermination (sect. 177a) if the perpetrators are Austrian citizens, but as to nuclear weapons only so far as the offence did not be committed by order or at the responsibility of a contracting party of the treaty against the distribution of nuclear weapons, Federal Law Gazette Nr. 258/1970, which is a state with nuclear weapons;
5. hijacking (sect. 185) and criminal offences against life and limb in this connection or against the freedom of aviation and its intentional endangering (sect. 186) if
 - a) the criminal offence is directed against an Austrian aircraft,
 - b) the aircraft lands in Austria and the perpetrators are still on board;
 - c) the aircraft has been rented out to someone without a crew who has his business seat in Austria or – in default of such a seat resides permanently in Austria; or
 - d) the perpetrator is in Austria and cannot be extradited;
6. other criminal offences for which Austria is bound to prosecution even if they have been committed abroad, irrespective of the laws which are valid for the scene of the crime;
7. criminal offences which commit an Austrian against an Austrian if both of them have their domicile or general residence in Austria;
8. participation (sect. 12) in a criminal offence which has been committed by the direct perpetrator at home as well as receiving stolen goods (sect. 164) and money laundering (sect. 165) referring to an offence being committed at home;
9. terrorist association (sect. 278b) and terrorist criminal offences (sect. 278c) as well as

criminal offences under sections 128 to 131, 144 and 145 and 223 to 224, which have been committed in this connection, if

- a) the perpetrator has been an Austrian at the time of the offence or he has gained the Austrian citizenship afterwards and is still in its possession at the time of the institution of penal proceedings;
 - b) the perpetrator has his domicile or general residence at home;
 - c) the offence has been committed in favour of a legal entity having its seat in Austria;
 - d) the offence has been committed against the National Parliament, the Federal Parliament, the Federal Assembly, the Federal Government, a Provincial Parliament, a Provincial Government, the Constitutional Court, the Administrative Court, the Supreme Court, any other court or administrative authority or against the people of the Republic of Austria;
 - e) the offence has been committed against an authority of the European Union or against an entity under the treaties for the institution of the European Communities or the treaty on the European Union, having its seat in the Republic of Austria;
 - f) the perpetrator has been a foreigner at the time of the offence, is now in Austria and cannot be extradited.
10. financing of terrorism (sect. 278d) if
- a) the perpetrator has been an Austrian at the time of the offence or he has gained the Austrian citizenship afterwards and is still in its possession at the time of the institution of penal proceedings; or
 - b) the perpetrator has been a foreigner at the time of the offence, is now in Austria and cannot be extradited.

(2) If the penal laws mentioned in para. 1 cannot be applied only for the reason that there has been committed a criminal offence which is punished by a severer sanction, the offence being committed abroad shall be punished nevertheless irrespective of the penal laws which are valid for the scene of the crime pursuant to the Austrian penal laws.

Criminal offences committed abroad which are subject to prosecution only if they are liable to persecution according to the laws which are valid for the scene of the crime

Section 65 (1) For other criminal offences committed abroad than those referred to in sections 63 and 64 applies the Austrian criminal law, if the offences are also liable to persecution according to the laws which are valid for the scene of the crime:

1. if the offender has been Austrian at the time of the offence or if he has acquired Austrian citizenship at a later date and if he still holds citizenship at the time of initiation of the criminal proceedings;
 2. if the offender has been a foreigner at the time of the offence, was found out inland and can not be extradited to a foreign state for other reasons than the nature or characteristics of the offence.
- (2) The penalty is to be determined so that the perpetrator in general is not treated less favorably than he would have been according to the laws of the state where he committed the offence.
- (3) It is sufficient that the offence is liable to persecution according to Austrian law if there is no penal power at the place where the criminal act was committed.
- (4) The punishability ceases to exist:
1. if the punishability of the offence has been extinct according to the laws which are valid for the scene of the crime;
 2. if the offender has been acquitted or the prosecution has been abandoned by a court of the state, in which the offence had been committed;
 3. if the offender has been sentenced legally binding by a foreign court and if the penalty has been executed totally or in case that the penalty has not been executed, if the penalty acceptilata has been acceptilated or if the enforceability has been time-barred according to the foreign law;
 4. as long as the enforceability of the penalty imposed by the foreign court is set out totally or partially.

If the preconditions apply, preventive sanctions according to Austrian laws have to be disposed against an Austrian person, even if this person cannot be punished inland according to the reasons mentioned in the previous paragraph.

Other definitions

Section 74 (1) In the sense of this Federal Law means

1 to 7...

8. computer system: single as well as combined devices which serve automation-aided data-processing.

(2) Personal data and non-personal data as well as computer programs are to be understood as data in the meaning of this federal law.

Unlawful access to a Computer system

Section 118a (1) A person who, with the intent to obtain information on data for himself or for another unauthorized person, which are stored in a computer system not being destined for him, and to make them available to another person for whom they are not destined by using them or making them public, and to procure in this way an economic gain for himself or another person or causing a disadvantage for another person, obtains the access to a computer system or to a part of such a system for which he is not permitted to dispose or not to dispose alone, by violating specific safety precautions within the computer system, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) The offender is to be prosecuted only with the consent of the aggrieved party.

Infringement of the secrecy of telecommunications

Section 119 (1) A person who, with the intent to obtain information not being destined for himself on communications transmitted through a telecommunication sect. 3 n.13 of the Telecommunication Act) or a computer system for himself or for another unauthorized person, attaches technical means to the telecommunication device or the computer system or otherwise prepares such means to receive information and makes use of them, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) The offender is to be prosecuted only with the consent of the aggrieved party.

Unlawful interception of data

Section 119a (1) A person who, with the intent to obtain information on data for himself or for another unauthorized person, which are transmitted by a computer system not destined for him, and to make them available to another person for whom they are not destined by using them or making them public, and to procure in this way an economic gain for himself or another person or causing a disadvantage for another person, attaches technical means to the computer system or otherwise prepares such means to receive information and makes use of them, or intercepts the electromagnetic radiation of a computer system, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) The offender is to be prosecuted only with the consent of the aggrieved party.

Damaging of data

Section 126a (1) A person who causes damage to another person by altering, erasing or otherwise rendering useless or suppressing automation-aided processed, transmitted or entrusted data without being authorized to dispose of the data or to dispose of them alone, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) A person who causes damage exceeding 2.000 Euro by the offence is to be sentenced to imprisonment up to two years or to pay a fine up to 360 day-fines; a person who causes damage exceeding 40.000 Euro is to be sentenced to imprisonment from 6 months to five years.

Interference with the functioning of a Computer system

Section 126b A person who interferes seriously with the functioning of a computer system for which he is not permitted to dispose or to dispose alone by feeding or transmitting data is to be sentenced, in case the offence is not punishable under section 126a, to imprisonment up to six months or to pay a fine up to 360 day-fines.

Misuse of computer programs and access data

Section 126c (1) Whoever produces, introduces, distributes, sells or otherwise makes accessible

1. a computer program or a comparable equipment which has been obviously created or adapted due to its particular nature to commit an unlawful access to a computer system (sect. 118a), an infringement of the secrecy of telecommunications (sect. 119), an unlawful interception of data (sect. 119a), a damaging of data (sect. 126a) or an interference with the functioning of a computer system (sect. 126b), or

2. a computer pass word, an access code or comparable data rendering possible the access to a computer system or a part of it, with the intent that they will be used for the commitment of any criminal offence mentioned in para.1, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) A person shall not be punished under para. 1 who prevents voluntarily that the computer program mentioned in para. 1 or the comparable equipment or the pass word, the access code or the comparable data will not be used in a way mentioned in sections 118a, 119, 119a, 126a or 126b. If there is no danger of such a use or if it has been removed without an activity of the offender, he shall not be punished in case he, unaware of that fact, makes voluntarily and seriously an effort to remove it.

Fraudulent misuse of data processing

Section 148a (1) A person who, with the intent to enrich himself or a third person unlawfully, causes economic damage to another's property by influencing the result of automation-aided data processing through arrangement of the program, input, alteration or erasure of data (sect. 126a para. 2) or through other interference with the course of data processing, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) A person who commits this offence professionally or causes damage exceeding 2.000 Euro is to be sentenced to imprisonment up to three years, a person who causes damage by committing the offence exceeding 40.000 Euro is to be sentenced to imprisonment from one year to ten years.

Falsification of data

Section 225a A person who produces false data by input, alteration, erasure or suppression of data or falsifies authentic data with the intent for using them legally as evidence of a right, legal relationship or fact is to be sentenced to imprisonment up to one year.

Appendix 2: Federal Law on Copyright in Work of Literature and Art and on Related Rights

Infringement

Section 91 (1) Any person who commits an infringement of the kind referred to sections 86 para. 1, 90b, 90c para. 1 or 90d para. 1 shall be liable to imprisonment not exceeding six month or to a fine not exceeding 360 times the daily rate. The infringement shall not, however, be punishable if it only involves the unauthorized reproduction or an unauthorized recording of a recitation or a performance for personal use or for the personal use of another person effected free of charge.

(1a) cancelled

(2) Any person who, as the owner or director of an enterprise, does not prevent an infringement of this kind (para. 1 and para. 1a) from being committed within the activities of the enterprise by an employee or agent shall also be liable to penalty.

(2a) Any person who by way of trade commits an offence under para.1. 1a or 2 shall be liable to imprisonment not exceeding two years.

(3) The offender shall be prosecuted only at the request of the person whose right has been infringed.

(4) Section 85 para. 1, 3 and 4 on publication of judgements shall apply *mutatis mutandis*.

(5) The criminal proceedings shall be heard by the judge of the court of first instance sitting alone.

Appendix 3: Austrian Telecommunications Act 2003

Confidentiality of the communications, data protection General

Section 92. (1) Unless otherwise provided by this Federal Act, the provisions of the Data Protection Act 2000 [Datenschutzgesetz], BGBl. I no. 165/1999, shall apply to the facts regulated in this Federal Act.

(2) The provisions of the Code of Criminal Procedure [StPO], BGBl. no. 631/1975, shall remain unaffected by the provisions of this section.

(3) Irrespective of § 3, in this section the term

1. "provider" means an operator of public communications services;
2. "user" means any natural person using a publicly available communications service, for private or business purposes, without necessarily having subscribed to this service;
3. "master data" means all personal data required for the establishment, processing, modification or termination of the legal relations between the user and the provider or for the production and publication of subscriber directories, including
 - a) surname and first name,
 - b) academic degree,
 - c) residential address,
 - d) subscriber number and other contact information for the communication,
 - e) information on type and contents of the contractual relationship,
 - f) financial standing;
4. "traffic data" means any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof;
- 4a. "access data" means the traffic data created at the operator during access by a subscriber to a public communications network and required for assignment to the subscriber of the network addresses used for a communication at a specific point of time;
5. "content data" means the contents of conveyed communications (item 7);
6. "location data" means any data processed in a communications network, indicating the geographic position of the telecommunications terminal equipment of a user of a publicly available communications service;
7. "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available communications service. This does not include any information conveyed as part of a broadcasting service to the public over a communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;
8. "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;
9. "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;
10. "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Subscriber directory

Section 103. (1) The operator may use and evaluate the data included in the subscriber directory pursuant to § 69 (3) and (4) only for the purposes of using the publicly available telephone service. Any other usage shall not be permitted. In particular, data must not be used to create electronic profiles of subscribers or to categorise these subscribers, except for the preparation and publication of subscriber directories. The operator shall make it more difficult to copy electronic subscriber directories, according to the state of the art and economic reasonableness.

(2) Transmission of data contained in a subscriber directory to the persons specified in § 18 (1) item 4 shall be permitted taking into account § 69 (5).

(3) The restriction of use under subsection (1) shall apply to data transmitted under subsection (2).

(4) The provisions of the foregoing subsections on the permitted use, evaluation and transmission of data relating to a subscriber shall not apply to court requests referring to the clearing up and prosecution of a specific criminal offence. By making technical and organisational arrangements the operator shall ensure that such requests can be complied with also in terms of data not entered pursuant to § 69 (5).

Appendix 4: Austrian E-Commerce Act

Definitions

Section 3. In the terms of this Federal Act:

1. "**information society service**" shall mean a service normally provided in return for consideration electronically by distance selling at the individual retrieval of the recipient (§ 1(1)2 of the Notification Act of 1999), particularly the online marketing of goods and services, online information offers, online advertising, electronic search engines and data enquiry options as well as services which transmit information via an electronic network and provide access to such a network or store the information of a user;
2. "**service provider**" shall mean a natural or legal person or other institution with legal capacity which provides an information society service;
3. "**established service provider**" shall mean any provider who effectively pursues an economic activity using a fixed establishment for an indefinite period, whereby the presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;
4. "**user**" shall mean any natural or legal person or other institution with legal capacity which uses an information society service for professional or other purposes, particularly in order to obtain information or make information available;
5. "**consumer**" shall mean any natural person who acts for purposes which are outside his or her trade, business or profession;
6. "**commercial communication**" shall mean advertising and other forms of communication designed to promote, directly or indirectly, the sale of goods and services or the image of a company, except:
 - a) information allowing direct access to the activity of the company, e.g. a domain name or an electronic-mail address; as well as
 - b) information relating to the goods, services or image of a company, compiled in an independent manner, particularly when this is without financial consideration;
7. "**Member State**" shall mean any member state of the European Community or of the Agreement Establishing a European Economic Area;
8. "**co-ordinated field**" shall mean the general and specific legal provisions applicable to information society services and service providers concerning the taking up of such activity, particularly legal provisions on the qualification and conduct of service providers, on authorisation or notification, and on the quality and content of the information society services, including the provisions applicable to advertising and contracts, and concerning the legal responsibility of service providers.

Appendix 5: Federal Statute on Responsibility of Entities for Criminal Offences

Responsibility of Entities – Provisions relating to Substantive Law Responsibility

Section 3. (1) Subject to the additional conditions defined in paragraphs 2 or 3 an entity shall be responsible for a criminal offence if

1. the offence was committed for the benefit of the entity or
 2. duties of the entity have been neglected by such offence.
- (2) The entity shall be responsible for offences committed by a decision maker if the decision maker acted illegally and culpably.
- (3) The entity shall be responsible for criminal offences of staff if
1. the facts and circumstances which correspond to the statutory definition of an offence have been realised in an illegal manner; the entity shall be responsible for an offence that requires wilful action only if a staff has acted with wilful intent, and for a criminal offence that requires negligent action only if a staff has failed to apply the due care required in the respective circumstances; and
 2. commission of the offence was made possible or considerably easier due to the fact that decision makers failed to apply the due and reasonable care required in the respective circumstances, in particular by omitting to take material technical, organisational or staff-related measures to prevent such offences.
- (4) Responsibility of an entity for an offence and criminal liability of decision makers or staff on grounds of the same offence shall not exclude each other.

Fine for the entity

Section 4. (1) If an entity is responsible for a criminal offence, a fine shall be imposed.

(2) The fine shall be assessed in the form of daily rates. The fine shall amount to at least one daily rate.

(3) The number of daily fines shall be up to

180

- if the criminal penalty for the offence is a life sentence or imprisonment of up to twenty years,

155

- if the criminal penalty for the offence is imprisonment of up to fifteen years,

130

- if the criminal penalty for the offence is imprisonment of up to ten years,

100

- if the criminal penalty for the offence is imprisonment of up to five years,

85

- if the criminal penalty for the offence is imprisonment of up to three years,

70

- if the criminal penalty for the offence is imprisonment of up to two years,

55

- if the criminal penalty for the offence is imprisonment of up to one year,

40

- in all other cases.

(4) The daily rate shall be assessed on the basis of the income situation of the entity by taking into account its other financial performance. The daily rate shall be equal to one 360th of the yearly proceeds or exceed or fall short of such amount by not more than one third; however, the daily rate shall amount to not less than 50 euros and not more than 10.000 euros. If the association serves charitable, humanitarian or church purposes (Sections 34 to 47 Fiscal Code, BGBl. No. 194/1961) or is not profit-oriented, the daily rate shall be fixed at a minimum of 2 euros and a maximum of 500 euros.

Appendix 6: Federal Law on Extradition and Mutual Assistance in Criminal Matters

Reciprocity

Section 3. (1) A foreign request shall only be complied with provided that it is guaranteed that the requesting State would also comply with a similar request by Austria.

(2) A request may not be filed under this law by an Austrian authority if a similar request by another State were not able to be complied with, except in the event that a request appears to be needed urgently for specific reasons. In this case the requested State shall be notified of the lack of reciprocity.

(3) In the event of doubt over observance of reciprocity, the opinion of the Federal Minister of Justice shall be sought.

(4) Another State may be guaranteed reciprocity in connection with a request made under this law, provided that no intergovernmental agreement exists and that it would be permissible under this law to comply with a similar request of this State.

Jurisdiction for Processing Letters Rogatory

Section 55. (1) The district court is competent to process letters rogatory, sections 2 and 3 notwithstanding; in cases where under the 1975 Code of Criminal Procedure, the decision is reserved for the *Ratskammer* or in which there is a request for a search, seizure, temporary injunction or a decision under section 145a of the Code of Criminal Procedure, the court of justice of the first instance in whose district the mutual assistance procedure is to be brought has jurisdiction. Sections 23 and 24 of the 1988 Youth Court Act are applicable as appropriate. If approval of cross-border observation is sought, the court of justice of the first instance in whose district the border will probably be crossed has jurisdiction; in case of observation in an aircraft that flies into Austria, however, the court of justice in whose district the landing site is located has jurisdiction. Information about a criminal procedure, execution of a prison sentence or preventive measures is issued by the court with jurisdiction; for requests for the transfer of records, the office in which the records are kept has jurisdiction. If a person detained in the prison of a court of justice is to be interrogated, that court of justice has jurisdiction. If the jurisdiction cannot be determined according to these rules, the District Court of the Inner City of Vienna, in cases in which the decision is reserved for the court of justice of the first instance, the Regional Criminal Court of Vienna has jurisdiction.

(2) If a person to be transferred is in prison or preventive custody, the decision on the request for transfer is made by a single judge of the court given in section 16 of the Penal Sentence Enforcement Act, otherwise it is the court on whose order the detention is based. The Federal Ministry of Justice is to be informed of this decision. The Federal Minister of Justice must refuse the transfer if one of the circumstances listed in sections 2 and 3 (1) is present. Transfer at the appropriate border crossing or any other transfer site agreed to be performed by police officers of the Ministry of Justice.

(3) If a person detained in another state is to be transferred through Austria to a third state for important investigative activities, in particular their interrogation or confrontation, sections 44, 47 and 49 apply as appropriate.

Applicable Procedures

Section 58. Mutual assistance is to be provided according to the provisions for criminal procedures within Austria. A request to follow a specific deviating procedure will be granted if this procedure is consistent with the principles of Austrian criminal procedure. If mutual assistance is provided in the form of confiscation (section 143 of the 1975 Code of Criminal Procedure) or a temporary injunction (section 144a of the 1975 Code of Criminal Procedure), this is to be limited in time; the foreign authority making the request is to be informed in the appropriate way.

Appendix 7: Code of Criminal Procedure¹

Monitoring of a Telecommunication

Section 149a

- (1) For the purposes of this Federal Law Gazette means
1. "monitoring of a telecommunication"
 - a) the establishment of the premises where a final device being characterized by a certain subscriber's line is situated or has been situated,
 - b) the establishment what subscriber's lines are or have been the origin or the destination of a telecommunication,
 - c) the listening, interception, controlling, recording and any other monitoring with regard to the contents of information being transmitted or received through telecommunication,
 2. "result of the monitoring of a telecommunication" any data of origin, transmission or contents which is acquired by it,
 3. "distributor's line" the address which characterizes the technical device being the origin or destination of a telecommunication.
- (2) Monitoring of a telecommunication is admissible
1. if it is to expect that by this means the clearing up of an intentionally committed penal offence being punished by a prison sentence for a term exceeding six months can be promoted and the holder of the distributor's line expressly agrees to the monitoring,
 2. in the cases of para. 1 n.1 let).a) and b) also if it is to expect that by this means the clearing up of an intentionally committed penal offence being punished by a prison sentence for a term exceeding one year can be promoted and particulars of the suspect can be established by such monitoring.
 3. in the cases of para. 1 n.1 let).c) also if monitoring seems to be necessary for the clearing up of an intentionally committed penal offence being punished by a prison sentence for a term exceeding one year and
 - a) the holder of the distributor's line is highly suspected in person to have committed the offence, or
 - b) there are reasons to believe that a person being highly suspected of the offence will use the distributor's line or will establish a connection with it.
- (3) Monitoring of a distributor's line under para. 2 n. 2 and 3
1. whose holder is a media entrepreneur (sect. 1 n.6 of the Media Act) is only admissible if it is to expect that by this means the clearing up of a penal offence can be promoted which is punished by life imprisonment or by a prison sentence for a minimum term of five years and a maximum term exceeding ten years,
 2. whose holder is a person being exempted from the obligation to state as a witness under sect.152 para. 1 n.4 or 5 (sect. 152 para. 3) is only admissible if this person himself is highly suspected of the offence.
- (4) Monitoring is only admissible if the proportionality for the purpose of the measure is observed. In this connection it shall be particularly taken into consideration that the aimed success is justifiably proportionate to the presumably effected infringement upon the rights of disinterested third parties and it shall be examined whether there could be also a reasonable chance of the aimed success by taking less incisive measures.

¹ An English version of the relevant sections of the revised Code of Criminal Procedure is currently not available.