Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 30 May 2007
[Reformat in March 2011]

Cybercrime legislation – country profile

AUSTRIA

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

Comments may be sent to:

Economic Crime Division
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
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)* *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).
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data*":* For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;* c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Section 74 para. 1 subpara. 8 and para. 2 of the Austrian Penal Code (include the definition of "computer system" and "computer data")** 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. **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.** **Section 3.** In the terms of this Federal Act: 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; **Section 92 para. 3 subpara. 4 of the Austrian Telecommunications Act 2003 (include the definition of "traffic data")** **Section 92** (3) Irrespective of § 3, in this section the term 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;
Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Section 118a of the Austrian Penal Code** **Unlawful access to a Computer system** (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.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Section 119 and 119a of the Austrian Penal Code** **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.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Section 126a of the Austrian Penal Code** **Damaging of data** (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.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Section 126b of the Austrian Penal Code** **Interference with the functioning of a Computer system** 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.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted	**Section 126c of the Austrian Penal Code** **Misuse of computer programs arid access data** (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

primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	(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.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Section 225a of the Austrian Penal Code** **Falsification of data** 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.
Article 8 – Computer-related fraud	**Section 148a of the Austrian Penal Code**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Fraudulent misuse of data processing** (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.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all	Section 207a of the Austrian Penal Code

persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Section 91 of the Federal Law on Copyright in Work of Literature and Art and on Related Rights** **Infringement** (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 herd by the judge of the court of first instance sitting alone.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting	**Section12 and 15 of the Austrian Penal Code**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**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 committal 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.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Section 3 of the Federal Statute on Responsibility of Entities for Criminal Offences (*Verbandsverantwortlichkeitsgesetz - VbVG*)** **Responsibility of Entities – Provisions relating to Substantive Law Responsibility** (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 staffrelated 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.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	Article 13 paragraph 1: 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; Article 13 paragraph 2: Section 4 of the Federal Statute on Responsibility of Entities for Criminal Offences
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention;	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.

b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other	See comment to Article 14.

independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	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 Subscriber directory** (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).
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:	See comment to Article 16.

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**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** **Confidentiality of the communications, data protection** **General** **Section 92.** (3) Irrespective of § 3, in this section the term 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; 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; **Subscriber directory** **Section 103.**

	(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).
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures	Section 109 et seq., 119 to 122 of the revised Code of Criminal Procedure (in force from 2008-1-1)

referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Section 134 and 137 of the revised Code of Criminal Procedure (in force from 2008-1-1)
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability:	See comment to Article 20

i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its	**Sections 64 and 65 of the Austrian Penal Code** **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;

territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	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 acceptilate 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.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.	Direct applicability of the Convention upon its ratification by Austria

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent	Direct applicability of the Convention upon its ratification by Austria; with regard to the non-extradition and subsequent prosecution of Austrian nationals see also

possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	Section 65 para. 1 subpara. 1 of the Austrian Penal Code **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;
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such	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

information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**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.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and	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

requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the	**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.

execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:	Direct applicability of the Convention upon its ratification by Austria

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or	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) **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.

similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	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 **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.

Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	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 **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.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	Direct applicability of the Convention upon its ratification by Austria
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	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 **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.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	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 **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.
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.	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.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	