www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Version August 2016

Cybercrime legislation – country profile

Germany

This profile has been prepared within the framework of capacity building programmes of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest 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:

Cybercrime Division
Directorate General of Human Rights and Rule of Law
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:	**Germany**
Signature of Convention:	23/11/2001
Ratification/accession:	09/03/2009

Provisions of the Convention	
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	**"Computer system" and "computer data"** Under German law, there is no general definition of the terms "computer system", "computer data". However for the purposes of sections 202a, 202b, 202c, 202d, 303a and 303b of the German Criminal Code " data" are defined as those which are only stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable. **"Service provider"** Pursuant to point 6 of Section 3 of the Telecommunications Act (TKG), "service provider" (Diensteanbieter) means anybody who, on a fully or partially commercial basis a) provides telecommunications services, or b) is involved in the provision of such services. **"Traffic data"** Pursuant to point 30 of Section 3 of the Telecommunications Act (TKG), traffic data are data collected, processed or used in the provision of a telecommunications service.
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.	**<u>Section 202a German Criminal Code - Data espionage</u>** (1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine. (2) Within the meaning of subsection (1) above data shall only be those stored

	or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.
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 202b German Criminal Code** Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.
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 303a German Criminal Code - Data tampering** (1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine. (2) The attempt shall be punishable.
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 303b German Criminal Code - Computer sabotage** (1) Whosoever interferes with data processing operations which are of substantial importance to another by 1. committing an offence under section303a(1); or 2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or 3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, shall be liable to imprisonment not exceeding three years or a fine. (2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine. (3) The attempt shall be punishable. (4) In especially serious cases under subsection (2) above the penalty shall be

	imprisonment from six months to ten years. An especially serious case typically occurs if the offender 1. causes major financial loss, 2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or 3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.
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 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,	**<u>Section 202c German Criminal Code - Acts preparatory to data espionage and phishing</u>** (1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible 1. passwords or other security codes enabling access to data (section 202a(2)), or 2. software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding one year or a fine.

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.	
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 269 German Criminal Code - Forgery of data intended to provide proof** (1) Whosoever for the purposes of deception in legal commerce stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner, shall be liable to imprisonment not exceeding five years or a fine. (2) The attempt shall be punishable. (3) Section 267(3) and (4) German Criminal Code shall apply mutatis mutandis. **Section 267 German Criminal Code - Forgery** (1)… (2)… (3) In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender 1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of fraud or forgery; 2. causes major financial loss; 3. substantially endangers the security of legal commerce through a large number of counterfeit or falsified documents; or 4. abuses his powers or his position as a public official. (4) Whosoever commits forgery on a commercial basis as a member of a gang whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269 shall be liable to imprisonment from one to ten years, in less serious cases to imprisonment from six months to five years.

Article 8 – Computer-related fraud 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.	**<u>Section 263a German Criminal Code - Computer fraud</u>** (1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine. (2) Section 263(2) to (7) shall apply mutatis mutandis. (3) Whosoever prepares an offence under subsection (1) above by writing computer programs the purpose of which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment not exceeding three years or a fine. According to Section 263a para. 2 German Criminal Code Section 263 para. 2 to para. 7 of the German Criminal Code shall apply mutatis mutandis: **Section 263 German Criminal Code – Fraud** (1) … (2) … (3) In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender 1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of forgery or fraud; 2. causes a major financial loss of or acts with the intent of placing a large number of persons in danger of financial loss by the continued commission of offences of fraud; 3. places another person in financial hardship; 4. abuses his powers or his position as a public official; or 5. pretends that an insured event has happened after he or another have for this purpose set fire to an object of significant value or destroyed it, in whole or in part, through setting fire to it or caused the sinking or beaching of a ship. (4) … (5) Whosoever on a commercial basis commits fraud as a member of a gang,

	whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269 shall be liable to imprisonment from one to ten years, in less serious cases to imprisonment from six months to five 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 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.	**<u>Section 184b German Criminal Code - Distribution, acquisition, and possession of child pornography</u>** (1) Whosoever 1. disseminates child pornography or makes it accessible to the general public; whereby pornographic written materials (section 11 (3)) shall be deemed to be child pornography if they relate to: a) sexual activities performed by, on or in the presence of a person under the age of fourteen years (child), b) the reproduction of a child in a state of full or partial undress in a posture unnaturally displaying sexual characteristics, or c) the lascivious reproduction of the unclothed genitalia or the unclothed buttocks of a child, 2. undertakes to obtain possession for another of child pornography reproducing an actual or realistic activity, 3. produces child pornography reproducing an actual activity, or 4. produces, obtains, supplies, stocks, offers, commends, or undertakes to import or export child pornography in order to use such child pornography, or copies made from such material, within the meaning of numbers 1 or 2 above or of section 184d (1), first sentence, or to facilitate such use by another, inasmuch as the offence is not liable to punishment pursuant to number 3, shall be liable to imprisonment from three months to five years. (2) In the cases under subsection (1) above, the penalty shall be imprisonment of six months to ten years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and if, in the cases of subsection (1) numbers 1, 2, and 4, the written material reproduces an actual or realistic activity. (3) Whosoever undertakes to obtain possession of child pornography

	reproducing an actual or realistic activity, or whosoever possesses such material, shall be liable to imprisonment not exceeding three years or a fine. (4) The attempt shall be punishable; this shall not apply to offences pursuant to subsection (1) numbers 2 and 4 as well as offences pursuant to subsection (3). (5) Subsection (1) number 2 and subsection (3) above shall not apply to acts that exclusively serve the fulfilment of the following: 1. state functions, 2. tasks resulting from agreements with a governmental agency having competence, or 3. official or professional duties. (6) In the cases under subsection (2) above, section 73d shall apply. Objects to which an offence under subsection (1) numbers 2 or 3 or subsection (3) above relates shall be subject to a deprivation order. Section 74a shall apply. **Section 184c German Criminal Code - Distribution, acquisition, and possession of juvenile pornography** (1) Whosoever 1. disseminates juvenile pornography or makes it accessible to the general public; whereby pornographic written materials (section 11 (3)) shall be deemed to be juvenile pornography if they relate to: a) sexual activities performed by, on or in the presence of a person who has reached the age of fourteen but is not yet eighteen years of age, or b) the reproduction of a person fourteen years of age but not yet eighteen years of age in a state of full or partial undress in a posture unnaturally displaying sexual characteristics, 2. undertakes to obtain possession for another of juvenile pornography reproducing an actual or realistic activity, 3. produces juvenile pornography reproducing an actual activity or 4. produces, obtains, supplies, stocks, offers, commends, or undertakes to import or export juvenile pornography in order to use such juvenile pornography, or copies made thereof, within the meaning of numbers 1 or 2 above or of section 184d (1), first sentence, or to facilitate such use by another,

	unless the offence is liable to punishment pursuant to number 3, shall be liable to imprisonment not exceeding three years or to a fine. (2) In the cases under subsection (1) above, the penalty shall be imprisonment of three months to five years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and if, in the cases of subsection (1) numbers 1, 2, and 4, the written material reproduces an actual or realistic activity. (3) Whosoever undertakes to obtain possession of juvenile pornography reproducing an actual activity, or whosoever possesses such material, shall be liable to imprisonment not exceeding two years or a fine. (4) Subsection (1) number 3, also in conjunction with subsection (5), and subsection (3), are not to be applied to acts by persons relating to such juvenile pornography that they have produced exclusively for their personal use with the consent of the persons depicted. (5) The attempt shall be punishable; this shall not apply to offences pursuant to subsection (1) numbers 2 and 4 as well as pursuant to subsection (3). (6) Section 184b subsections (5) and (6) shall apply mutatis mutandis.
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,	**Article 106 German Act on Copyright and Related Rights - Unlawful exploitation of copyrighted works** (1) Anyone who without the consent of the rightholder reproduces, distributes or communicates to the public a work or an adaptation or transformation of a work in manners other than those permitted by law shall be liable to imprisonment of not more than 3 years or a fine. (2) Any attempt shall be punishable. **Article 107 German Act on Copyright and Related Rights - Unlawful affixing of designation of author**

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.	(1) Any person who 1. without the consent of the author affixes to the original of an artistic work the designation of author (Article 10 (1)) or distributes an original bearing such designation, 2. affixes to a copy, an adaptation or transformation of an artistic work the designation of author (Article 10 (1)) in a manner which gives the copy, adaptation or transformation the appearance of an original, or distributes a copy, such an adaptation or transformation bearing such designation, shall be liable to imprisonment of not more than three years or a fine, unless other provisions impose a more serious sentence. (2) Any attempt shall be punishable. **Article 108 German Act on Copyright and Related Rights - Infringement of related rights** (1) Any person who without the consent of the rightholder 1. reproduces, distributes or communicates to the public a scientific edition (Article 70) or an adaptation or transformation of such an edition, 2. exploits a posthumous work or an adaptation or transformation of such a work contrary to Article 71, 3. reproduces, distributes or communicates to the public a photograph (Article 72) or an adaptation or transformation of a photograph, 4. exploits a performance by a performer contrary to Article 77 (1) or (2), first sentence, Article 78 (1), 5. exploits an audio recording contrary to Article 85, 6. exploits a broadcast contrary to Article 87, 7. exploits a video recording or a video and audio recording contrary to Articles 94 or 95 read in conjunction with Article 94, 8. exploits a database contrary to Article 87b (1), in manners other than those permitted by law shall be liable to imprisonment of not more than three years or a fine. (2) Any attempt shall be punishable.

	Article 108a German Act on Copyright and Related Rights - Unlawful exploitation on a commercial scale (1) Where the offender in the cases referred to in Articles 106 to 108 acts on a commercial basis, the penalty shall be imprisonment of not more than five years or a fine. (2) Any attempt shall be punishable. **Article 108b German Act on Copyright and Related Rights -Infringement of technological measures and rights-management information** (1) Any person who, 1. with the intention of enabling for himself or a third party access to a work which is protected under this Act or to other subject-matter protected under this Act or its exploitation, circumvents an effective technological measure without the consent of the rightholder, or 2. knowingly without authorisation a) removes or alters rights-management information provided by rightholders, if any of the information concerned is affixed to a copy of a work or of other protected subject-matter, or is released in the context of the communication to the public of such a work or protected subject-matter, or b) distributes, imports for distribution, broadcasts, communicates to the public or makes available to the public a work or other protected subject-matter where rights-management information was removed or altered without authorisation by doing so, has at least carelessly induced, enabled, facilitated or concealed an infringement of copyright or related rights, if the offence was not committed exclusively for the personal private use of the offender or of persons personally associated with the offender or does not relate to such use, shall be liable to imprisonment of not more than one year or a fine. (2) Punishment shall also be imposed on any person who in violation of Article 95a (3) produces, imports, distributes, sells or rents a device, a product or component for commercial purposes. (3) If in cases under paragraph (1) the offender acts on a commercial scale, the penalty shall be imprisonment of not more than three years or a fine.

Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 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.	**Section 23 German Criminal Code - Liability for attempt** (1) Any attempt to commit a felony entails criminal liability; this applies to attempted misdemeanours only if expressly so provided by law. (2) An attempt may be punished more leniently than the completed offence (section 49(1)). **Section 27 German Criminal Code - Aiding** (1) Any person who intentionally assists another in the intentional commission of an unlawful act shall be convicted and sentenced as an aider. (2) The sentence for the aider shall be based on the penalty for a principal. It shall be mitigated pursuant to section 49(1). **Section 26 German Criminal Code - Abetting** Any person who intentionally induces another to intentionally commit an unlawful act (abettor) shall be liable to be sentenced as if he were a principal.
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	**Section 30 German Act on Regulatory Offences - Regulatory Fine Imposed on Legal Persons and on Associations of Persons** (1) Where someone acting 1. as an entity authorised to represent a legal person or as a member of such an entity, 2. as chairman of the executive committee of an association without legal capacity or as a member of such committee, 3. as a partner authorised to represent a partnership with legal capacity, or 4. as the authorised representative with full power of attorney or in a managerial position as procura-holder or the authorised representative with a commercial power of attorney of a legal person or of an association of persons referred to in numbers 2 or 3, 5. as another person responsible on behalf of the management of the operation or enterprise forming part of a legal person, or of an association of persons

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.	referred to in numbers 2 or 3, also covering supervision of the conduct of business or other exercise of controlling powers in a managerial position, has committed a criminal offence or a regulatory offence as a result of which duties incumbent on the legal person or on the association of persons have been violated, or where the legal person or the association of persons has been enriched or was intended to be enriched, a regulatory fine may be imposed on such person or association. (2) The regulatory fine shall amount 1. in the case of a criminal offence committed with intent, to not more than ten million Euros, 2. in the case of a criminal offence committed negligently, to not more than five million Euros. Where there has been commission of a regulatory offence, the maximum regulatory fine that can be imposed shall be determined by the maximum regulatory fine imposable for the regulatory offence concerned. If the Act refers to this provision, the maximum amount of the regulatory fine in accordance with the second sentence shall be multiplied by ten for the offences referred to in the Act. The second sentence shall also apply where there has been commission of an act simultaneously constituting a criminal offence and a regulatory offence, provided that the maximum regulatory fine imposable for the regulatory offence exceeds the maximum pursuant to the first sentence. **Section 130 German Act on Regulatory Offences - Violation of Obligatory Supervision in Operations and Enterprises** (1) Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties incumbent on the owner and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision. The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel. (2) An operation or undertaking within the meaning of subsection 1 shall include

	a public enterprise. (3) Where the breach of duty carries a criminal penalty, the regulatory offence may carry a regulatory fine not exceeding one million Euros. Section 30 subsection 2 third sentence shall be applicable. Where the breach of duty carries a regulatory fine, the maximum regulatory fine for breach of the duty of supervision shall be determined by the maximum regulatory fine imposable for the breach of duty. The third sentence shall also apply in the case of a breach of duty carrying simultaneously a criminal penalty and a regulatory fine, provided that the maximum regulatory fine imposable for the breach of duty exceeds the maximum pursuant to the first sentence.
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.	The level of the sanctions and measures for the several offences follows form the answers to the Articles 2 to 11 see above and concerning legal persons from Article 12.
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; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal	See below (Articles 16 – 21)

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 independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.	See below (Articles 16 – 21)

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.	In accordance with Sections 94 and 98 of the Code of Criminal Procedure stored data may be secured by seizing the storage media. This requires that a criminal offence is suspected. Further, the fact that the data may be of importance as evidence for the investigation must be substantiated. As a rule, seizing storage media requires that a court order has been issued. In exigent circumstances, seizure may also be ordered by the public prosecutor's office and the police (first sentence of Section 98(1), Code of Criminal Procedure). Sections 94 and 98 of the Code of Criminal Procedure do not apply to measures aiming to obtain traffic data from a provider of telecom services; in such cases, Section 100g of the Code of Criminal Procedure will apply (see Article 18). With regard to subscriber data, a provider of telecom services is legally obliged to record such data according to the Telecommunications Act.
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: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the	With regard to traffic data, preservation will be – to a certain extent – generally mandatory according to the Act introducing a Storage Obligation and a Maximum Storage Period for Traffic Data, which entered into force on 18 December 2015. The act lays down a storage period for traffic data, which are defined more closely in the Telecommunications Act, of four or ten weeks.

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.	Stored traffic data may be requested in accordance with Section 100g of the Code of Criminal Procedure (see below, Section 18).
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.	Article 18 (1) lit. a: Instead of seizing the storage media, stored data can be obtained by an order to produce the relevant storage media according to Section 95 Code of Criminal Procedure. The collection of subscriber information in the form of customer data, including a subscriber's name and address and assigned subscriber numbers and identification codes, is permitted in the case of telecommunications undertakings, provided that this is required for investigation of the case or determination of the suspect's whereabouts (Section 100j, Code of Criminal Procedure). This applies only if - as in the case of all criminal procedural measures - there is an initial suspicion of a criminal offence. A court order is not required. Article 18 (1) lit. b: Traffic data may be obtained through a production order in accordance with Section 100g Code of Criminal Procedure. In case of Section 100g (1) of the above Code, with regard to traffic data retained for business purposes (as opposed to mandatorily retained traffic data, see below), this requires the suspicion of either - a criminal offence which qualifies as significantly important - not only with regard to the general definition of the offence in question (which would particularly apply to offences listed in Section 100a (2) of the Code of Criminal

	Procedure), but also with regard to the circumstances of the individual case – - or a criminal offence using telecommunications has been committed. If the measure refers to mandatorily retained traffic data (see Article 17), collection is permitted only in the case of particularly serious criminal offences within the meaning of the offences listed in Section 100g (2) of the above Code. In all both cases of traffic data collection, a court order is required as rule. Only in urgent cases of urgency which do not concern mandatorily retained data (Section 100g (2) of the above Code) the order can be issued by a public prosecutor. The police may not issue the by itself, not even in cases of urgency.
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	Article 19 (1), (3) is covered by section 94: Storage data may be searched during a search at the premises where it is physically located. The search itself requires that (1) a criminal offence is suspected and (2) that the search aims at the apprehension of the accused or that it is presumed that the search will lead to the discovery of evidence. If the search takes place at premises other than those of the accused, it is only admissible if certain facts support the conclusion that the person, trace, or object sought is located on the premises to be searched. (3) In general, a search requires a prior search warrant issued by a court. In exigent circumstances, the search may also be ordered by the public prosecutor's office and the police. Section 110 (1) of the Code of Criminal Procedure explicitly allows of the public prosecutor and, if he so orders, the officials assisting him (section 152 of the Courts Constitution Act), to examine documents (including those in electronic form) belonging to the person affected by the search.

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 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 19 (2) Under Section 110 (3) of the Code of Criminal Procedure, the examination of an electronic storage medium at the premises concerned by a search may be extended also to cover physically separate storage media insofar as they are accessible from the storage medium if there is reason to fear that the data sought would otherwise be lost. The aim of the provision is to prevent the loss of data constituting evidence which, although accessible from the examined computer, are on a physically separate storage medium such as the server on the intranet or internet. This also includes emails which are stored on the provider's server. Examination is permitted if there is reason to fear that data or evidence would otherwise be lost, i.e. if the external storage medium cannot be secured in good time. If data relevant to the proceedings are found, they may be secured pursuant to the second sentence of Section 110(3) of the Code of Criminal Procedure.
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.	Traffic data may also be obtained in real time based on Section 100g (1) of the Code of Criminal Procedure. This provision does not only apply to traffic data already being stored (either for business purposes or due to the legal obligation imposed by the Act introducing a Storage Obligation and a Maximum Storage Period for Traffic Data, which entered into force on 18 December 2015, see Article 17), but also allows to collect traffic data in real time. The legal requirements are the same as set out in relation to Section 100g (1) Code of Criminal Procedure above (see Article 18).

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.	
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: 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.	Content data can be collected in real time by means of interception of telecommunications under Sections 100a and 100b of the Code of Criminal Procedure. This requires that a serious criminal offence listed in Section 100a (2) of the Code is suspected and that interception pursuant to Section 100b has been ordered by a court. In cases of urgency, interception can be ordered by a public prosecutor. In that case, the measure has to be terminated unless a court confirms it within three working days. The police may not order interception by itself, not even in cases of urgency. Provided all of these requirements are fulfilled, authorities may apply several techniques, ranging from • traditional telephone interception to • techniques typically applied in cybercrime related cases, such as – surveillance of data traffic on computers with internet access or internet servers and – seizing e-mails from a service provider. For production orders concerning stored traffic data, see Article 18.
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	**Section 3 German Criminal Code**

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 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.	Offences committed on the territory of the Federal Republic of Germany German criminal law shall apply to acts committed on German territory. **<u>Section 4 German Criminal Code</u>** Offences committed on German ships and aircraft German criminal law shall apply, regardless of the law applicable in the locality where the act was committed, to acts committed on a ship or an aircraft entitled to fly the federal flag or the national insignia of the Federal Republic of Germany. **<u>Section 7 German Criminal Code</u>** Offences committed abroad—other cases (1) … (2) German criminal law shall apply to other offences committed abroad if the act is a criminal offence at the locality of its commission or if that locality is not subject to any criminal law jurisdiction, and if the offender: 1. was German at the time of the offence or became German after the commission [2. was a foreigner at the time of the offence, is discovered in Germany and, although the Extradition Act would permit extradition for such an offence, is not extradited because a request for extradition within a reasonable period of time is not made, is rejected, or the extradition is not feasible.]
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	It was not necessary to explicitly implement the provisions of chapter III into German national law, because the general legal basis on which German authorities can cooperate already allows for the full extent of international cooperation as foreseen in these provisions. Even where no international treaties exist, the Act on International Cooperation in Criminal Matters enables German authorities to perform measures foreseen in the German Code of Criminal Procedure also in execution of a request for MLA. This involves the measures specifically mentioned in this chapter. Furthermore under German law the provisions of chapter III apply directly as far as they are in force in relation to the requesting country. This ensures, that all

provided for under such arrangement or treaty shall apply. 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	specific features and conditions of these provisions are taken into account.
Article 25 – General principles relating to mutual assistance	

1 The Parties shall afford one another mutual assistance to the widest extent 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.	see above
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	see above

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.	
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 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	see above

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 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: 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.	see above
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;	see above

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 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.	see above
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.	see above
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,	see above

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.	
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.	see above
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.	see above
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	Bundeskriminalamt, Fachbereich SO42-1 SO 42 (High Technology Crime) Working Languages: German, English Bundeskriminalamt National High Tech Crime Unit (SO42) Phone Number: +49-611-5513101 24/7 Phone Number: +49-611-5513101 Fax Number: +49-611-5545100

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. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	E-mail: so42-cyber@bka.bund.de (for non-emergency use only); so42-officeronduty@bka.bund.de (for emergency use only) Address: Bundeskriminalamt, Thaerstr. 11 65193 Wiesbaden, Germany
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.	