

Cybercrime legislation – country profile

Germany

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

Comments may be sent to:

Alexander Seger
Head of the Economic Crime Division
Department of Technical Cooperation
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

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

Version 22 Jul 10

Country:	Germany
Signature of Convention:	Yes: 23 November 2001
Ratification/accession:	Yes: 09 March 2009
Provisions of the Convention	
<i>Chapter I – Use of terms</i>	
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	While German law does not provide for a definition of a "computer system" other than referring to "data processing systems" in Section 303b of the German Criminal Code (see Article 5 below), "computer data" are covered (yet not defined) by Section 202a (2) of the Criminal Code (Strafgesetzbuch), 2009 ("StGB")¹: Section 202a Data espionage (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 of not more than 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. "Service provider" is covered in part by Section 3 of the German Telecommunications Code (Telekommunikationsgesetz), 2010 ("TKG") and in part by Section 2 of the German Telecommunications Media Code (Telemediengesetz), 2010 ("TMG"): Section 3 TKG Definitions Within the meaning of this law is or are 1. [...] 6. "service provider" anyone who, all or part commercially, a) provides telecommunication services or b) contributes in doing so. Section 2 TMG
--	--

¹ All English versions of German legal texts, though not representing official translations, have been taken from official sources (<http://www.gesetze-im-internet.de>) except for the Telecommunications Code (TKG), the Telecommunications Media Code (TMG), the Law on Copyright and Neighbouring Rights (UrhG), the Administrative Offenses Act (OWiG) and the Act on International Legal Assistance in Criminal Matters (IRG).

	Definitions Within the meaning of this law 1. a service provider is any natural or legal person, who stores own or alien telecommunication media for usage, or who mediates access for usage; [...] "Traffic data" are covered by Section 3 of the German Telecommunications Code (Telekommunikationsgesetz), 2010 ("TKG"): Section 3 Definitions Within the meaning of this law is or are 1. [...] 30. "traffic data" such data which is collected, processed or made use of by the supply of a telecommunication service.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
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.	German Criminal Code (Strafgesetzbuch), 2009 ("StGB"): Section 202a Data espionage (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 of not more than 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	German Criminal Code (Strafgesetzbuch), 2009 ("StGB"): Section 202b Phishing

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.	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 of not more than 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.	German Criminal Code (Strafgesetzbuch), 2009 (“StGB”): Section 303a Data tampering (1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment of not more than two years or a fine. (2) The attempt shall be punishable. (3) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.
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.	German Criminal Code (Strafgesetzbuch), 2009 (“StGB”): Section 303b Computer sabotage (1) Whosoever interferes with data processing operations which are of substantial importance to another by 1. committing an offence under section 303a (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 of not more than 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 of not more than 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 populations supply with vital goods or services or the national security of the Federal Republic of Germany. (5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.
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	German Criminal Code (Strafgesetzbuch), 2009 ("StGB"): Section 202c Acts preparatory to data espionage and phishing (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 of not more than one year or a fine. (2) Section 149 (2) and (3) shall apply mutatis mutandis. Section 149 Preparatory acts

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.	(1) Whosoever prepares to counterfeit money or stamps by producing, procuring for himself or another, offering for sale, storing or giving to another 1. plates, frames, type, blocks, negatives, stencils, computer programs or similar equipment which by its nature is suitable for the commission of the offence; 2. paper, which is identical or easy to confuse with the type of paper designated for the production of money or official stamps and especially protected against imitation; or 3. holograms or other elements affording protection against counterfeiting shall be liable to imprisonment of not more than five years or a fine if he prepared to counterfeit money, otherwise with imprisonment of not more than two years or a fine. (2) Whosoever voluntarily 1. gives up the commission of the offence prepared for and averts a danger caused by him that others continue to prepare the offence or commit it, or prevents the completion of the offence; and 2. destroys or renders unusable the means for counterfeiting, to the extent that they still exist and are useful for counterfeiting, or reports their existence to a public authority or surrenders them there, shall not be liable under subsection (1) above. (3) If the danger that others continue to prepare or commit the offence is averted, or the completion of the act prevented regardless of the contribution of the offender his voluntary and earnest efforts to achieve this aim shall suffice in lieu of subsection (2) No 1 above.
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.	German Criminal Code (Strafgesetzbuch), 2009 (“StGB”): Section 269 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 of not more than five years or a fine. (2) The attempt shall be punishable. (3) Section 267 (3) and (4) shall apply mutatis mutandis.

	Section 267 Forgery (1) Whosoever for the purpose of deception in legal commerce produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be liable to imprisonment of not more than five years or a fine. (2) The attempt shall be punishable. (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	German Criminal Code (Strafgesetzbuch), 2009 ("StGB"): Section 263a Computer fraud (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 of not more than 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

right, an economic benefit for oneself or for another person.	another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment of not more than three years or a fine. (4) In cases under subsection (3) above section 149 (2) and (3) shall apply mutatis mutandis. Section 263 Fraud (1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by causing or maintaining an error by pretending false facts or by distorting or suppressing true facts shall be liable to imprisonment of not more than five years or a fine. (2) The attempt shall be punishable. (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) Section 243 (2), section 247 and section 248a shall apply mutatis mutandis. (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.
--	---

	(6) The court may make a supervision order (section 68 (1)). (7) Section 43a and 73d shall apply if the offender acts as a member of a gang whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269. section 73d shall also apply if the offender acts on a commercial basis.
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	German Criminal Code (Strafgesetzbuch), 2009 (“StGB”): Section 184b Distribution, acquisition and possession of child pornography (1) Whosoever 1. disseminates; 2. publicly displays, presents, or otherwise makes accessible; or 3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of children (section 176 (1)) (child pornography) shall be liable to imprisonment from three months to five years. (2) Whosoever undertakes to obtain possession for another of child pornography reproducing an actual or realistic activity shall incur the same penalty. (3) In cases under subsection (1) or subsection (2) 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 the child pornography reproduces an actual or realistic activity. (4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment of not more than two years or a fine. Whosoever possesses the written materials set forth in the 1st sentence shall incur the same penalty. (5) Subsections (2) and (4) above shall not apply to acts that exclusively serve the fulfilment of lawful official or professional duties. (6) In cases under subsection (3) above section 73d shall apply. Objects to which an offence under subsection (2) or (4) above relates shall be subject to a deprivation order. section 74a shall apply.

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.	Section 184c Distribution, acquisition and possession of juvenile pornography (1) Whosoever 1. disseminates; 2. publicly displays, presents, or otherwise makes accessible; or 3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of persons between the ages of fourteen to eighteen years (juvenile pornography) shall be liable to imprisonment of not more than three years or a fine. (2) Whosoever undertakes to obtain possession for another of juvenile pornography reproducing an actual or realistic activity shall incur the same penalty. (3) In cases under subsection (1) or subsection (2) 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 the juvenile pornography reproduces an actual or realistic activity. (4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment of not more than one year or a fine. The 1st sentence shall not apply to acts of persons related to juvenile pornography produced by them while under eighteen years of age and with the consent of the persons therein depicted. (5) Section 184b (5) and (6) shall apply mutatis mutandis. Section 184d Distribution of pornographic performances by broadcasting, media services or telecommunications services Whosoever disseminates pornographic performances via broadcast, media services, or telecommunications services shall be liable pursuant to sections 184 to 184c. In cases under section 184 (1) the 1st sentence above shall not apply to dissemination via media
--	--

	services or telecommunications services if it is ensured by technical or other measures that the pornographic performance is not accessible to persons under eighteen years of age.
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	Law on Copyright and Neighbouring Rights, 2007 ("UrhG"): Section 106 Unauthorized Exploitation of Copyrighted Works (1) Whoever reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work, other than in a manner allowed by law and without the right holder's consent, shall be punished with imprisonment for up to three years or a fine. (2) An attempt shall be punishable. Section 107 Unlawful Affixing of Designation of Author (1) Whoever 1. without the author's consent, affixes a designation of author (section 10 subsection (1)) to the original of a work of fine art or distributes an original bearing such designation, 2. affixes a designation of author (section 10 subsection (1)) on a copy, adaptation or transformation of a work of fine art in such manner as to give to the copy, adaptation or transformation the appearance of an original or distributes a copy, adaptation or transformation bearing such designation, shall be punished with imprisonment for up to three years or a fine provided the offence is not subject to a more severe penalty under other provisions. (2) An attempt shall be punishable. Section 108 Infringement of Neighboring Rights (1) Whoever, other than in a manner allowed by law and without the right holder's consent: 1. reproduces, distributes or publicly communicates a scientific edition (section 70) or an

obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	adaptation or transformation of such edition; 2. exploits a posthumous work or an adaptation or transformation of such work contrary to section 71; 3. reproduces, distributes or publicly communicates a photograph (section 72) or an adaptation or transformation of a photograph; 4. exploits a performance contrary to section 77 subsection (1) or (2) or section 78 subsection (1); 5. exploits an audio recording contrary to section 85; 6. exploits a broadcast contrary to section 87; 7. exploits a video or video and audio recording contrary to section 94 or section 95 in conjunction with section 94; 8. uses a database contrary to section 87b (1), shall be punished with imprisonment for up to three years or a fine. (2) An attempt shall be punishable. Section 108a Unlawful Exploitation on a Commercial Basis (1) Where the person committing the acts referred to in sections 106 to 108 does so on a commercial basis, the penalty shall be imprisonment for up to five years or a fine. (2) An attempt shall be punishable. Section 108b [Unauthorised interference with technical protection measures and information necessary for rights management] (1) Any person who, 1. with the intention of enabling access to or use of a work protected under this Act or other subject matter protected under this Act, circumvents an effective technical measure without the consent of the right holder, or 2. knowingly without authorisation a) removes or alters rights management information originating from right holders, if any such information is affixed to a reproduction of a work or other protected subject matter or is published in connection with the public communication of such a work or other
--	--

	protected subject matter, or (b) disseminates, prepares for dissemination, broadcasts, publicly communicates or makes available to the public a work or other protected subject matter where rights management information has been removed or altered without authorisation and in so doing has at least recklessly induced, enabled, facilitated or concealed the infringement of copyright or related rights shall, if the offence was not committed for the exclusive private use of the perpetrator or persons personally associated with the perpetrator or is not related to such use, be punished with imprisonment for no more than one year or a fine. (2) Punishment shall also be imposed upon any person who, in violation of section 95a subsection (3), produces, imports, disseminates, sells or rents a device, product or component for commercial purposes. (3) Where the person committing the acts referred to in subsection (1) does so on a commercial basis, the penalty shall be imprisonment for no more than three years or a fine.
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	German Criminal Code (Strafgesetzbuch), 2009 (“StGB”): Section 22 Definition (Attempt) A person attempts to commit an offence if he takes steps which will immediately lead to the completion of the offence as envisaged by him. Section 23 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)). (3) If the offender due to gross ignorance fails to realise that the attempt could under no circumstances have led to the completion of the offence due to the nature of its object or the means by which it was to be committed, the court may order a discharge, or mitigate the sentence as it sees fit (section 49 (2)).

	Section 24 Withdrawal (1) A person who of his own volition gives up the further execution of the offence or prevents its completion shall not be liable for the attempt. If the offence is not completed regardless of his actions, that person shall not be liable if he has made a voluntary and earnest effort to prevent the completion of the offence. (2) If more than one person participate in the offence, the person who voluntarily prevents its completion shall not be liable for the attempt. His voluntary and earnest effort to prevent the completion of the offence shall suffice for exemption from liability, if the offence is not completed regardless of his actions or is committed independently of his earlier contribution to the offence. Section 26 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. Section 27 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).
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	Administrative Offences Act, 2007 ("OWiG"): Section 30 Regulatory fine imposed on legal entities and associations of persons

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.	(1) Where a person 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 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 one million Euros, 2. in the case of a criminal offence committed negligently, to not more than five hundred thousand Euros. Where a regulatory offence has been committed, the maximum regulatory fine that can be imposed shall be determined by the maximum regulatory fine imposable for the regulatory offence at issue. The second sentence shall also apply where an act simultaneously constituting a criminal offence and a regulatory offence has been committed, provided that the maximum regulatory fine imposable for the regulatory offence exceeds the
--	---

	maximum pursuant to the first sentence. (3) Section 17 subsection 4 and section 18 shall apply <i>mutatis mutandis</i>. (4) If criminal proceedings or proceedings to impose a regulatory fine are not instituted in respect of the criminal offence or the regulatory offence, or if such proceedings are discontinued, or if imposition of a criminal penalty is dispensed with, the regulatory fine may be assessed independently. Statutory provision may be made to the effect that a regulatory fine may be imposed in its own right in further cases as well. However, independent assessment of a regulatory fine against the legal person or association of persons shall be precluded where the criminal offence or the regulatory offence cannot be prosecuted for legal reasons; section 33 subsection 1, second sentence, shall remain unaffected. (5) Assessment of a regulatory fine incurred by the legal person or association of persons shall, in respect of one and the same offence, preclude a forfeiture order, pursuant to sections 73 or 73a of the Criminal Code or pursuant to section 29a, against such person or association of persons. Section 130 Violation of obligatory supervision in firms 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 as such 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. 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 second 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.	Article 13 (1) is covered by the above-mentioned Articles (Sections 202a, 202b, 202c, 263a, 269, 303a, 303a StGB and Sections 106, 107, 108, 108a, 108b UrhG). Article 13 (2) is covered by Section 30 OWiG (see Article 12 above).
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:	See below (Articles 16-21).

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 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, <i>inter alia</i>, include judicial or other 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.	See below (Articles 16-21).
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may	German Code of Criminal Procedure (Strafprozessordnung), 2008 (“StPO”): With respect to computer data, Article 16 is covered by Sections 94, 95 and 98 StPO.

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 94 [Objects Which May Be Seized] (1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured. (2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily. (3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation. Section 95 [Obligation to Surrender] (1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request. (2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify. Section 98 [Order of Seizure] (1) Seizure may be ordered only by the judge and, in exigent circumstances, by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to Section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court. (2) An official who has seized an object without a judicial order shall apply for judicial approval within 3 days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a judicial decision. As long as no public charges have been preferred, the decision shall be made by the court of competency pursuant to Section 162 subsection
--	--

	(1). Once public charges have been preferred, the decision shall be made by the court dealing with the matter. The person concerned may also submit the application to the Local Court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights. (3) Where after public charges have been preferred, the public prosecution office or one of the officials assisting has effected seizure, the court shall be notified of the seizure within 3 days; the objects seized shall be put at its disposal. (4) If it is necessary to effect seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such seizure. The agency making the request shall be entitled to participate. No such request shall be necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces. With respect to traffic data, Article 16 is covered by Section 100g StPO. Section 100g [Information on Telecommunications Connections] (1) If certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory, 1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence or 2. has committed a criminal offence by means of telecommunication; then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is
--	--

	proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1. (2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply <i>mutatis mutandis</i>. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult. (3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process. (4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying: 1. the number of proceedings during which measures were implemented pursuant to subsection (1); 2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders; 3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence; 4. the number of months elapsed during which telecommunications call data was intercepted, measured from the time the order was made; 5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable. Section 100a [Conditions regarding Interception of Telecommunications] (1) [...] (3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection. Section 100b
--	--

	[Order to Intercept Telecommunications] (1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry. (2) The order shall be given in writing. The operative part of the order shall indicate: 1. where known, the name and address of the person against whom the measure is directed, 2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment. 3. the type, extent and duration of the measure specifying the time at which it will be concluded. (3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply <i>mutatis mutandis</i>. (4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof. (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	Covered by Section 100g StPO (see Article 16 above).

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 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	Article 18 (1) lit. a is covered by Section 95 of the German Code of Criminal Procedure (Strafprozessordnung), 2008 ("StPO"): Section 95 [Obligation to Surrender] (1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request. (2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify. Article 18 (1) lit. b is covered by Sections 112 and 113 of the German Telecommunications Code (Telekommunikationsgesetz), 2007 ("TKG"): Section 112 Automated Information Procedure (1) Any person providing publicly available telecommunications services shall store, without

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.	undue delay, data collected under section 111 subsection (1), first and third sentences, and subsection (2) in customer data files in which the telephone numbers and quotas of telephone numbers allocated to other telecommunications service providers for further marketing or other use and, with regard to ported numbers, the current carrier portability codes, are also to be included. Section 111 subsection (1), third and fourth sentences, apply accordingly with regard to the correction of customer data files. In the case of ported numbers the telephone number and associated carrier portability code are not to be erased before expiry of the year following the date on which the telephone number was returned to the network operator to whom it had originally been allocated. The person with obligations shall ensure that 1. the Federal Network Agency can, at all times, retrieve from customer data files data for information requests from the authorities referred to in subsection (2) by means of automated procedures in the Federal Republic of Germany; 2. data can be retrieved using incomplete search data or searches made by means of a similarity function. The requesting authority is to consider, without undue delay, the extent to which it needs the data provided and erase, without undue delay, any data not needed. The person with obligations is to ensure by technical and organisational measures that no retrievals can come to his notice. (2) Information from the customer data files pursuant to subsection (1) shall be provided to 1. the courts and criminal prosecution authorities; 2. federal and state police enforcement authorities for purposes of averting danger; 3. the Customs Criminological Office and customs investigation offices for criminal proceedings and the Customs Criminological Office for the preparation and execution of measures under section 39 of the Foreign Trade and Payments Act; 4. federal and state authorities for the protection of the Constitution, the Military Counterintelligence Service and the Federal Intelligence Service; 5. the emergency service centres pursuant to section 108 and the service centre for the maritime mobile emergency number 124124; 6. the Federal Financial Supervisory Authority; and 7. the Customs Administration authorities for the purposes set forth in section 2 subsection (1) of the Undeclared Work Act via central inquiry offices, as stipulated in subsection (4), at all times, insofar as such information is needed to discharge their legal functions and the requests are submitted to the Federal Network Agency by means of automated procedures.
--	--

	(3) The Federal Ministry of Economics and Technology shall be empowered to issue, in agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, and with the consent of the German Bundesrat, a statutory order in which the following matters are regulated 1. the essential requirements in respect of the technical procedures for a) the transmission of requests to the Federal Network Agency; b) the retrieval of data by the Federal Network Agency from persons with obligations, including the data types to be used for the queries; and c) transmission by the Federal Network Agency to the requesting authorities of the data retrieved; 2. the security requirements to be observed; and 3. in respect of retrievals using incomplete search data and searches made by means of similarity functions for which specifications on the character sequences to be included in the search are provided by the Ministries contributing to the statutory order, a) the minimum requirements in respect of the scope of the data to be entered in order to identify, as precisely as possible, the person to whom the search relates; b) the permitted number of hits to be transmitted to the requesting authority; and c) the requirements in respect of the erasure of data not needed. In other respects, the statutory order may also restrict the query facility for the authorities referred to in subsection (2) numbers 5 to 7 to the extent that is required for such authorities. The Federal Network Agency shall determine the technical details of the automated retrieval procedure in a technical directive to be drawn up with the participation of the associations concerned and the authorised bodies and to be brought into line with the state of the art, where required, and published by the Federal Network Agency in its Official Gazette. The person with obligations according to subsection (1) and the authorised bodies are to meet the requirements of the technical directive not later than one year following its publication. In the event of an amendment to the directive, defect-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect. (4) At the request of the authorities referred to in subsection (2), the Federal Network Agency shall retrieve and transmit to the requesting authority the relevant data sets from the customer data files pursuant to subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with the authorities referred to in subsection (2). For purposes of data protection control by the
--	---

	competent body, the Federal Network Agency shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, the person retrieving the data, the requesting authority and the reference number of the requesting authority. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year. (5) The person with obligations according to subsection (1) shall make all such technical arrangements in his area of responsibility as are required for the provision of information under this provision, at his expense. This also includes procurement of the equipment required to secure confidentiality and protection against unauthorised access, installation of a suitable telecommunications connection, participation in the closed user system and the continued provision of all such arrangements as are required under the statutory order and the technical directive pursuant to subsection (3). Compensation for information provided by means of automated procedures is not paid to persons with obligations. Section 113 Manual Information Procedure (1) Any person commercially providing or assisting in providing telecommunications services shall, in a given instance, provide the competent authorities, at their request, without undue delay, with information on data collected under sections 95 and 111 to the extent required for the prosecution of criminal or regulatory offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Military Counterintelligence Service. The person with obligations pursuant to sentence 1 shall provide information on data by means of which access to terminal equipment or to storage devices or units installed in such equipment or in the network is protected, notably personal identification numbers (PINs) or personal unlocking keys (PUKs), by virtue of an information request pursuant to section 161 subsection (1), first sentence, or section 163 subsection (1) of the Code of Criminal Procedure, data collection provisions in federal or state police legislation for averting danger to public safety or order, section 8 subsection (1) of the Federal Act on the Protection of the Constitution, the corresponding provisions of legislation to protect the constitutions of the <i>Länder</i>, section 2 subsection (1) of the Federal Intelligence Service Act or section 4 subsection (1) of the Military Counterintelligence Service Act; such data shall not be transmitted to any other public or
--	---

	private bodies. Access to data which are subject to telecommunications privacy shall be permitted only under the conditions of the relevant legislation. The person with obligations shall maintain silence vis-à-vis his customers and third parties about the provision of information. (2) The person with obligations according to subsection (1) is to make such arrangements as are required in his area of responsibility for the provision of information, at his expense. In respect of information provided, the person with obligations is granted compensation by the requesting authority, the level of which, in derogation of section 23 of the Court Remuneration and Compensation Act, is determined by the statutory order referred to in section 110 subsection (9). Sentence 2 also applies in those cases in which, under the manual information procedure, merely data are requested which the person with obligations also keeps available for retrieval under the automated information procedure under section 112. Sentence 2 does not apply in those cases in which the information was not provided completely or correctly under the automated information procedure under section 112.
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.	Article 19 (1) and (3) are covered by Sections 94, 95, 102, 103, 105, 161 and 163 of the German Code of Criminal Procedure (Strafprozessordnung), 2008 ("StPO"): Section 94 [Objects Which May Be Seized] (1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured. (2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily. (3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation. Section 95 [Obligation to Surrender] (1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request. (2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are

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 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.	entitled to refuse to testify. Section 102 [Search in Respect of the Suspect] A body search, a search of the property and of the private and other premises of a person who, as a perpetrator or as an inciter or accessory before the fact, is suspected of committing a criminal offence, or is suspected of accessoryship after the fact or of obstruction of justice or of handling stolen goods, may be made for the purpose of his apprehension, as well as in cases where it may be presumed that the search will lead to the discovery of evidence. Section 103 [Searches in Respect of Other Persons] (1) Searches in respect of other persons shall be admissible only for the purpose of apprehending the accused or to follow up the traces of a criminal offence or to seize certain objects, and only if certain facts support the conclusion that the person, trace, or object sought is located on the premises to be searched. For the purposes of apprehending an accused who is strongly suspected of having committed an offence pursuant to section 129a, also in conjunction with section 129b subsection (1), of the Criminal Code, or one of the offences designated in this provision, a search of private and other premises shall also be admissible if they are located in a building in which it may be assumed, on the basis of certain facts, that the accused is located. (2) The restrictions of subsection (1), first sentence, shall not apply to premises where the accused was apprehended or which he entered during the pursuit. Section 105 [Search Order; Execution] (1) Searches may be ordered only by the judge and, in exigent circumstances, also by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Searches pursuant to Section 103 subsection (1), second sentence, shall be ordered by the judge; in exigent circumstances the public prosecution office shall
--	--

	be authorized to order such searches. (2) Where private premises, business premises, or enclosed property are to be searched in the absence of the judge or the public prosecutor, a municipal official or two members of the community in the district of which the search is carried out shall be called in, if possible, to assist. The persons called in as members of the community may not be police officers or officials assisting the public prosecution office. (3) If it is necessary to carry out a search in an official building or in an installation or establishment of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such search. The requesting agency shall be entitled to participate. No such request shall be necessary if the search is to be carried out on premises which are inhabited exclusively by persons other than members of the Federal Armed Forces. Section 161 [Information and Investigations] (1) For the purpose indicated in Section 160 subsections (1) to (3), the public prosecution office shall be entitled to request information from all authorities and to make investigations of any kind, either itself or through the authorities and officials in the police force provided there are no other statutory provisions specifically regulating their powers. The authorities and officials in the police force shall be obliged to comply with the request or order of the public prosecution office and shall be entitled, in such cases, to request information from all authorities. (2) Where measures pursuant to this statute are only admissible where the commission of particular criminal offences is suspected, personal data that has been obtained as a result of a corresponding measure taken pursuant to another statute may be used as evidence in criminal proceedings without the consent of the person affected by the measure only to clear up one of the criminal offences in respect of which such a measure could have been ordered to clear up the offence pursuant to this statute. Section 100d, subsection (5), number 3 shall remain unaffected. (3) Personal data obtained in or from private premises by technical means for the purpose of personal protection during a clandestine investigation based on police law may be used as evidence, having regard to the principle of proportionality (Article 13 paragraph (5) of the Basic Law), only after determination of the lawfulness of the measure by the Local
--	---

	Court (Section 162 subsection (1)) in whose district the authority making the order is located; in exigent circumstances a judicial decision is to be sought without delay. Section 163 [Duties of the Police] (1) The authorities and officials in the police force shall investigate criminal offences and shall take all measures may not be deferred, in order to prevent concealment of facts. To this end they shall be entitled to request, and in exigent circumstances to demand, information from all authorities, as well as to conduct investigations of any kind insofar as there are no other statutory provisions specifically regulating their powers. (2) The authorities and officials in the police force shall transmit their records to the public prosecution office without delay. Where it appears necessary that a judicial investigation be performed promptly, transmission directly to the Local Court shall be possible. Article 19 (2) is covered Section 110 (3) StPO. Section 110 [Examination of Papers] (1) The public prosecution office and, if it so orders, the officials assisting it (section 152 of the Courts Constitution Act), shall have the authority to examine documents belonging to the person affected by the search. (2) In all other cases, officials shall be authorized to examine papers found by them only if the holder permits such examination. In all other cases they shall deliver any papers, the examination of which they deem necessary, to the public prosecution office in an envelope which shall be sealed with the official seal in the presence of the holder. (3) The examination of an electronic storage medium at the premises of the person affected by the search may be extended to cover also physically separate storage media insofar as they are accessible from the storage medium if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be secured; Section 98 subsection (2) shall apply <i>mutatis mutandis</i>.
--	---

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.	German Code of Criminal Procedure (Strafprozessordnung), 2008 (“StPO”): Section 100g [Information on Telecommunications Connections] (1) If certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory, 1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence or 2. has committed a criminal offence by means of telecommunication; then, to the extent that this is necessary to establish the facts or determine the accused’s whereabouts, traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused’s whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1. (2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply <i>mutatis mutandis</i>. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused’s whereabouts would offer no prospect of success or be much more difficult. (3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process. (4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying: 1. the number of proceedings during which measures were implemented pursuant to subsection (1); 2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
---	--

	3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence; 4. the number of months elapsed during which telecommunications call data was intercepted, measured from the time the order was made; 5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable. Section 100a [Conditions regarding Interception of Telecommunications] (1) [...] (3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection. Section 100b [Order to Intercept Telecommunications] (1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry. (2) The order shall be given in writing. The operative part of the order shall indicate: 1. where known, the name and address of the person against whom the measure is directed, 2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment. 3. the type, extent and duration of the measure specifying the time at which it will
--	---

	be concluded. (3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply <i>mutatis mutandis</i>. (4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof. (5) [...]
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	German Code of Criminal Procedure (Strafprozessordnung), 2008 (“StPO”): Section 100a [Conditions regarding Interception of Telecommunications] (1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if 1. certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, and 2. the offence is one of particular gravity in the individual case as well and 3. other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success. (2) Serious criminal offences for the purposes of subsection (1), number 1, are: 1. pursuant to the Criminal Code: a) crimes against peace, high treason, endangering the democratic Rule of Law, treason and endangering external security pursuant to sections 80 to 82, 84 to 86, 87 to 89 and 94 to 100a;

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.	b) bribery of a member of parliament pursuant to section 108e; c) crimes against the national defence pursuant to sections 109d to 109h; d) crimes against public order pursuant to sections 129 to 130; e) counterfeiting money and official stamps pursuant to sections 146 and 151, in each case in conjunction with section 152, as well as section 152a subsection (3) and section 152b subsections (1) to (4); f) crimes against sexual self-determination in the cases referred to in sections 176a, 176b, 177 subsection (2), number 2, and section 179 subsection (5), number 2; g) dissemination, purchase and possession of pornographic writings involving children and involving juveniles, pursuant to section 184b subsections (1) to (3), section 184c subsection (3);
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	h) murder and manslaughter pursuant to sections 211 and 212; i) crimes against personal liberty pursuant to sections 232 to 233a, 234, 234a, 239a and 239b; j) gang theft pursuant to section 244 subsection (1), number 2, and aggravated gang theft pursuant to section 244a; k) crimes of robbery or extortion pursuant to sections 249 to 255; l) commercial handling of stolen goods, gang handling of stolen goods and commercial gang handling of stolen goods pursuant to sections 260 and 260a; m) money laundering or concealment of unlawfully acquired assets pursuant to section 261 subsections (1), (2) and (4); n) fraud and computer fraud subject to the conditions set out in section 263 subsection (3), second sentence, and in the case of section 263 subsection (5), each in connection with section 263a subsection (2); o) subsidy fraud subject to the conditions set out in section 264 subsection (2), second sentence, and in the case of section 264 subsection (3), in conjunction with section 263 subsection (5); p) criminal offences involving falsification of documents under the conditions mentioned in section 267 subsection (3), second sentence, and in the case of section 267 subsection (4), in each case also in conjunction with section 268 subsection (5) or section 269 subsection (3), as well as pursuant to sections 275 subsection (2) and section 276 subsection (2); q) bankruptcy subject to the conditions set out in section 283a, second sentence; r) crimes against competition pursuant to section 298 and, subject to the conditions set

	out in section 300, second sentence, pursuant to section 299; s) crimes endangering public safety in the cases referred to in sections 306 to 306c, 307 subsections (1) to (3), section 308 subsections (1) to (3), section 309 subsections (1) to (4), section 310 subsection (1), sections 313, 314, 315 subsection (3), section 315b subsection (3), as well as sections 361a and 361c; t) taking and offering a bribe pursuant to sections 332 and 334; 2. pursuant to the Fiscal Code a) tax evasion under the conditions listed in section 370 subsection (3), second sentence, number 5; b) commercial, violent and gang smuggling pursuant to section 373; c) handling tax-evaded property as defined in section 374 subsection (2); 3. pursuant to the Pharmaceutical Products Act: criminal offences pursuant to section 95 subsection (1), number 2a, subject to the conditions listed in section 95 subsection (3), second sentence, number 2b; 4. pursuant to the Asylum Procedure Act: a) inducing an abusive application for asylum pursuant to section 84 subsection (3); b) commercial and gang inducement to make an abusive application for asylum pursuant to section 84a; 5. pursuant to the Residence Act: a) smuggling of aliens pursuant to section 96 subsection (2); b) smuggling resulting in death and commercial and gang smuggling pursuant to section 97; 6. pursuant to the Foreign Trade and Payments Act: criminal offences pursuant to section 34 subsections (1) to (6); 7. pursuant to the Narcotics Act: a) criminal offences pursuant to one of the provisions referred to in section 29 subsection (3), second sentence, number 1, subject to the conditions set out therein; b) criminal offences pursuant to sections 29a, 30 subsection (1), numbers 1, 2 and 4, as
--	--

	well as sections 30a and 30b; 8. pursuant to the Precursors Control Act: criminal offences pursuant to section 19 subsection (1), subject to the conditions set out in section 19 subsection (3), second sentence; 9. pursuant to the War Weapons Control Act: a) criminal offences pursuant to section 19 subsections (1) to (3) and section 20 subsections (1) and (2), as well as section 20a subsections (1) to (3), each also in conjunction with section 21; b) criminal offences pursuant to section 22a subsections (1) to (3); 10. pursuant to the Code of Crimes against International Law: a) genocide pursuant to section 6; b) crimes against humanity pursuant to section 7; c) war crimes pursuant to sections 8 to 12; 11. pursuant to the Weapons Act: a) criminal offences pursuant to section 51 subsections (1) to (3); b) criminal offences pursuant to section 52 subsection (1) numbers 1, 2c and 2d, as well as section 52 subsections (5) and (6). (3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection. (4) If there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired through a measure pursuant to subsection (1), the measure shall be inadmissible. Information concerning the core area of the private conduct of life which is acquired during a measure pursuant to subsection (1) shall not be used. Any records thereof shall be deleted without delay. The fact that they were obtained and deleted shall be documented.
--	--

Section 100b

[Order to Intercept Telecommunications]

(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry.

(2) The order shall be given in writing. The operative part of the order shall indicate:

1. where known, the name and address of the person against whom the measure is directed,
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment.
3. the type, extent and duration of the measure specifying the time at which it will be concluded.

(3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply *mutatis mutandis*.

(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.

(5) The *Länder* and the Federal Public Prosecutor General shall submit a report to the Federal Office of Justice every calendar year by the 30th June of the year following the reporting year, concerning measures ordered pursuant to Section 100a within their area of competence. The Federal Office of Justice shall produce a summary of the measures

	ordered nationwide during the reporting year and shall publish it on the Internet. (6) The reports pursuant to subsection (5) shall indicate: 1. the number of proceedings in which measures were ordered pursuant to Section 100a subsection (1); 2. the number of orders to intercept telecommunications pursuant to Section 100a subsection (1), distinguishing between a) initial and follow-up orders, as well as b) fixed, mobile and Internet telecommunication; 3. in each case the underlying criminal offence by reference to the categories listed in Section 100a subsection (2).
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,	German Criminal Code (Strafgesetzbuch), 2009 (“StGB”): Section 3 Offences committed on the territory of the Federal Republic of Germany German criminal law shall apply to acts committed on German territory. Section 4 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. Section 5 Offences committed abroad against domestic legal interests German criminal law shall apply, regardless of the law applicable in the locality where the act was committed, to the following acts committed abroad: 1. preparation of a war of aggression (section 80); 2. high treason against the Federation (sections 81 to 83); 3. endangering the democratic state under the rule of law (a) in cases under section 89 and section 90a (1), and section 90b, if the offender is German and has his main livelihood in the territory of the Federal Republic of Germany; and

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.	(b) in cases under section 90 and section 90a (2); 4. treason and endangering external national security (sections 94 to 100a); 5. offences against the national defence: (a) in cases under section 109 and sections 109e to 109g; and (b) in cases under section 109a, section 109d and section 109h, if the offender is German and has his main livelihood in the territory of the Federal Republic of Germany
5 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.	6. Causing the danger of political persecution (section 234a, section 241a) if the act is directed against a German who has his domicile or usual residence in Germany; 6a. abduction of minors in cases under section 235 (2) No 2, if the act is directed against a person who has his domicile or usual residence in Germany; 7. violation of business or trade secrets of a business physically located within the territory of the Federal Republic of Germany, or of an enterprise, which has its seat there, or of an enterprise with its seat abroad and which is dependent on an enterprise with its seat within the territory of the Federal Republic of Germany and which forms a group with the latter; 8. offences against sexual self-determination: (a) in cases under section 174 (1) and (3), if the offender and the victim are German at the time of the offence and have their main livelihood in Germany; and (b) in cases under sections 176 to 176b and section 182, if the offender is German; 9. abortion (section 218), if the offender at the time of the offence is German and has his main livelihood in the territory of the Federal Republic of Germany; 10. false testimony, perjury and false sworn affidavits (sections 153 to 156) in proceedings pending before a court or another German authority within the territory of the Federal Republic of Germany that has the authority to administer oaths or affirmations in lieu of oath; 11. offences against the environment under section 324, section 326, section 330 and section 330a committed within Germany's exclusive economic zone, to the extent that international conventions on the protection of the sea allow for their prosecution as criminal offences; 11a. offences under section 328 (2) Nos 3 and 4, (4) and (5), also in conjunction with section 330, if the offender is German at the time of the offence; 12. offences committed by a German public official or a person entrusted with special public service functions during their official stay or in connection with their official duties; 13. acts committed by a foreigner as a public official or as a person entrusted with special

	public service functions; 14. acts committed against public officials, persons entrusted with special public service functions, or soldiers in the Armed Forces during the discharge of their duties or in connection with their duties; 14a. bribing delegates (section 108e) if the offender is German at the time of the offence or the offence was committed vis-à-vis a German; 15. trafficking in human organs (section 18 of the Transplantation Act), if the offender is German at the time of the offence. Section 6 Offences committed abroad against internationally protected legal interests German criminal law shall further apply, regardless of the law of the locality where they are committed, to the following offences committed abroad: 1. <i>(repealed)</i>; 2. offences involving nuclear energy, explosives and radiation under section 307 and section 308 (1) to (4), section 309 (2) and section 310; 3. attacks on air and maritime traffic (section 316c); 4. human trafficking for the purpose of sexual exploitation, for the purpose of work exploitation and assisting human trafficking (sectionsection 232 to 233a); 5. unlawful drug dealing; 6. distribution of pornography under sections 184a, 184b (1) to (3) and section 184c (1) to (3), also in conjunction with section 184d, 1st sentence; 7. counterfeiting money and securities (section 146, section 151 and section 152), credit cards etc and blank eurocheque forms (section 152b (1) to (4)) as well as the relevant preparatory acts (sectionsection 149, 151, 152 and 152b (5)); 8. subsidy fraud (section 264); 9. offences which on the basis of an international agreement binding on the Federal Republic of Germany must be prosecuted even though committed abroad. Section 7 Offences committed abroad-other cases (1) German criminal law shall apply to offences committed abroad against a German, if the act is a criminal offence at the locality of its commission or if that locality is not subject to any criminal jurisdiction.
--	--

	(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; or 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. Section 8 Time of the offence An offence is deemed to have been committed at the time when the principal or the secondary participants acted, or, in the case of an omission, should have acted. The time when the result occurs is irrelevant. Section 9 Place of the offence (1) An offence is deemed to have been committed in every place where the offender acted or, in the case of an omission, should have acted, or in which the result if it is an element of the offence occurs or should have occurred according to the intention of the offender. (2) Acts of secondary participation are committed not only in the place where the offence was committed, but also in every place where the secondary participant acted or, in the case of an omission, should have acted or where, according to his intention, the offence should have been committed. If the secondary participant to an offence committed abroad acted within the territory of the Federal Republic of Germany, German criminal law shall apply to the secondary participation even though the act is not a criminal offence according to the law of the locality of its commission.
Chapter III – International co-operation Section 1 – General principles	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the	Article 24 is covered by Sections 2 and 3 of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 (“IRG”) in the absence of applicable international agreements:

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. 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.	Section 2 Principle (1) A foreign national who is being prosecuted or who has been sentenced in a foreign country because of an act punishable there may be extradited to such foreign country at the request of the competent authorities for the purpose of prosecution or execution of a sentence given because of that act or because of the imposition of another penalty. (2) A foreign national who has been sentenced in a foreign country because of an act punishable there may be extradited to another foreign country, which has taken over enforcement, at the request of the competent authorities of that country, for the purpose of executing the sentence imposed because of the act, or for the imposition of another penalty. (3) Foreign nationals pursuant to this law shall be persons who are not German nationals pursuant to Article 116 (1) of the Basic Law. Section 3 Extradition for the Purpose of Prosecution or Execution (1) Extradition shall be admissible only if the act contains the elements of a criminal offence under German law or if, after analogous conversion of the facts, the act would under German law constitute an offence. (2) Extradition for the purpose of prosecution shall be admissible only if the act is punishable under German law by a maximum of at least one year of imprisonment or if, after analogous conversion of the facts, the act would, under German law, be punishable by such a penalty. (3) Extradition for the purpose of execution shall be admissible only if extradition for the purpose of prosecution because of the act would have been allowed and if a penalty involving imprisonment is to be executed. It shall further be granted on condition if it is to be expected that the period of imprisonment to be served, or the sum of the periods of imprisonment still to be served, is at least four months.
---	--

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 that the details held on the register are correct at all times.	
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.	Article 25 is covered by provisions set forth in the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("IRG") in the absence of applicable international agreements, e.g. Sections 2, 3 (see above Article 24) and Sections 59 ff.: Section 59 Admissibility of Assistance (1) At the request of a competent authority of a foreign state, other legal assistance in a criminal matter may be provided. (2) Legal assistance within the meaning of subsection (1) shall be every type of aid given to foreign criminal proceedings regardless of whether the foreign proceedings are conducted by a court or by a governmental authority and whether the legal assistance is

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.	to be provided by a court or by a governmental authority. (3) Legal assistance may be provided only under circumstances under which German courts and governmental authorities could render legal assistance to each other.
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.	Section 60 Rendering Assistance If the governmental authority responsible for authorising legal assistance determines that the requirements for rendering legal assistance have been met, the governmental authority responsible for rendering the legal assistance shall be bound by such determination. Section 61 shall remain unaffected.
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 61 Court Decision (1) If a court decision that is responsible for rendering legal assistance considers that the requirements for rendering legal assistance have not been met, it shall give reasons for its opinion and shall request a ruling by the Higher Regional Court. The Higher Regional Court shall also rule upon application of the public prosecution office at the Higher Regional Court, or in the case of section 66, upon application of a person claiming that his rights would be violated if assistance were rendered, whether the requirements for rendering legal assistance have been met. For such proceedings before the Higher Regional Court, sections 30 and 31 subsections (1), (2) and (4), sections 32 and 33 subsections (1), (2) and (4), section 38 subsection (4), second sentence, and section 40 subsection (1), as well as the provisions of Chapter 11, Vol. 1 of the Code of Criminal Procedure, with the exception of sections 140-143, shall apply accordingly. For any subsequent proceedings, section 42 shall apply accordingly. (2) Jurisdiction <i>ratione loci</i> shall lie with the Higher Regional Court and the public prosecution office at the Higher Regional Court in whose district the legal assistance is to be or has been rendered. If acts of legal assistance are to be or have been carried out in the districts of different Higher Regional Courts, jurisdiction shall depend on which Higher Regional Court or, where no Higher Regional Court is yet involved in the case, which public prosecution office at a Higher Regional Court was first to deal with the case. (3) The decision of the Higher Regional Court shall be binding on those courts and authorities which are responsible for rendering the legal assistance. (4) Legal assistance may not be granted if the court has ruled that the requirements for

rendering legal assistance have not been met.

Section 62

Temporary Transfer to a Foreign Country for Foreign Proceedings

(1) A person who is held in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty within the territory to which this Act applies, may, on request by the competent authority of a foreign country, be temporarily transferred to that country to attend proceedings pending there to be examined as a witness, for the purpose of confrontation or for inspection by the court, if

1. after having been advised, he states that he consents and this is recorded by a judge,
2. it is not to be anticipated that the duration of deprivation of liberty will be extended or the purpose of the criminal proceedings will be prejudiced as a result of the transfer,
3. an assurance is given that during the period of his transfer, the person concerned will not be subjected to a penalty or other sanction or proceeded against by virtue of measures which could not also have been taken during his absence and that in the event of his release he may leave the requesting State, and
4. an assurance is given that the person concerned will be returned without delay following the taking of evidence unless this has been waived.

The consent (first sentence no. 1) cannot be revoked.

(2) The public prosecution office at the Higher Regional Court shall prepare and carry out the transfer. The public prosecution office at the Higher Regional Court in whose region the deprivation of liberty is being enforced shall have local jurisdiction.

(3) The period of deprivation of liberty served in the requesting State shall be deducted from the period of deprivation of liberty to be enforced within the territory to which this Act applies. Section 37 subsection (4) shall apply accordingly.

Section 63

Temporary Transfer from a Foreign Country for Foreign Proceedings

(1) A person who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty may, on request by the competent authority of that country, be temporarily transferred to the

	territory within which this law applies to give evidence for proceedings pending in that country and, after the evidence has been taken, be returned. The person concerned shall be kept in detention to ensure his return. (2) Detention shall be ordered by means of a written arrest warrant. The arrest warrant shall contain the following information: 1. the person concerned, 2. the request for the taking of evidence in the presence of the person concerned and 3. the reason for detention. (3) The decision concerning detention shall be taken by the judge responsible for rendering legal assistance or by the judge at the Local Court in whose district the authority responsible for rendering legal assistance is located. This decision is not open to appeal. (4) Sections 27, 45 subsection (4) and 62 subsection (2), first sentence, shall apply accordingly. Section 64 Transit of Witnesses (1) A foreign national who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty may, on request by a competent authority, be transported to a third state through the territory to which this law applies as a witness for examination, confrontation or inspection and be returned after the taking of evidence. (2) The person concerned will be kept in detention to ensure secure transit. Sections 27, 30 subsection (1), 42, 44, 45 subsections (3) and (4), 47, 63 subsection (2) shall apply accordingly. Section 65 Transit for Enforcement Purposes The transit of a foreign national, for purposes of enforcing a sentence or other sanction, from the state in which he was sentenced through the territory to which this law applies to a foreign country that has taken over such enforcement, shall be governed by sections 43 subsections (2) to (4) and sections 44, 45 and 47 as appropriate, provided that the request may also be submitted by a competent authority of the state in which the judgment was issued.
--	--

	Section 68 Return (1) A person sought who, on request and subject to his subsequent return, has been temporarily extradited to face criminal proceedings brought against him within the territory to which this law applies, shall be returned to the requested state at the agreed time unless that state waives his return. The public prosecution office involved in the criminal proceedings referred to in the first sentence shall be responsible for ordering and effecting the return of the person sought. (2) If the return of the person sought would not otherwise be guaranteed, his detention may be ordered by means of a written arrest warrant. The arrest warrant shall contain the following information: 1. the person sought, 2. the state to which the person sought is to be returned, and 3. the reasons justifying the order for detention. (3) The decision concerning detention shall be taken by the respective court competent for ordering measures involving deprivation of liberty in the criminal proceedings referred to in subsection (1), first sentence. The decision shall not be open to appeal. (4) Sections 18, 19, 24, 25, 27 and 45 subsection (4) shall apply accordingly. Section 69 Temporary Transfer from a Foreign Country for German Proceedings (1) A person who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty and who, on request, has been temporarily transferred to a German court or German authority for examination, confrontation or inspection shall, during his stay in the territory to which this law applies, be held in detention in order to ensure his return to that country. (2) The decision concerning detention shall be taken by the court seised with the case and, in respect of preparatory proceedings, by the judge at the Local Court in whose district the public prosecution office conducting the proceedings is located. The decision is not open to appeal.
Article 26 – Spontaneous information	Article 26 is covered by Sections 61a and 92 of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007

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 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.	("IRG") in the absence of applicable international agreements: Section 61a Transmission of Personal Data without Request (1) Courts and public prosecution offices may transmit personal data from criminal proceedings to the public authorities of another state as well as to interstate and supranational authorities without request by the latter if 1. transmission without request to a German court or to a German public prosecution office would have been admissible, 2. there are facts which warrant the expectation that the transmission is necessary a) in order to prepare a request by the receiving state for legal assistance for the purpose of prosecution or execution of a sentence for a crime that is punishable by a maximum of more than five years of imprisonment in the area of application of this law, and the conditions for granting assistance upon request would be met if such request were made, or b) in the individual case, to avert a danger to the existence or security of the state, or to the life, limb or freedom of a person, or to property of significant value, maintenance of which is demanded by the public interest, or to prevent a crime as described under letter a), and 3. the public authority to which the data are transmitted is competent to implement appropriate measures pursuant to number 2. If adequate data protection is ensured in the receiving state, number 2 letter a), first sentence, applies with the provision that a crime which is punishable by a maximum of more than five years of imprisonment at a place within the scope of application of this law is substituted by a crime of significant gravity. (2) Transmission is to be conducted under the condition that 1. time limits pursuant to German law for deletion and for review of deletion of transmitted data will be observed, 2. transmitted data will be used only for the purposes for which they were transferred, and 3. transmitted data will be deleted or corrected immediately upon information in accordance with subsection 4. Section 92 (former Section 83j)
---	--

	Transmission of Data without Request (1) To the extent provided by an international agreement, personal data that substantiate the suspicion that a criminal offence has been committed may be transmitted by public authorities to the public authorities of another European Union Member State as well as to organs and institutions of the European Communities, without request, provided that 1. a transmission, without request, to a German court or German public prosecution office would also be admissible and 2. the transmission is suited for a) the institution of criminal proceedings in that other Member State or b) the furthering of criminal proceedings already instituted in that Member State, and 3. the authority to which the data are transmitted is competent to undertake the measures under number 2. (2) section 61a subsections (2) to (4) shall apply accordingly.
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	Article 27 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 (“IRG”) in the absence of applicable international agreements, see Article 25 above.

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, <i>ordre public</i> 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.	Article 28 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("IRG") in the absence of applicable international agreements, see Article 25 above.

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.	
Section 2 – Specific provisions 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	Article 29 is covered by Sections 66 and 67 of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("IRG") in the absence of applicable international agreements: Section 66 Surrender of objects (1) Upon request by the competent authority of a foreign country, objects may be surrendered 1. which may serve as evidence for foreign proceedings or 2. which the person concerned or a participant acquired as a result of the offence on which the request is based or as consideration for such objects. (2) Surrender shall be admissible only if 1. the act giving rise to the request constitutes an unlawful act also under German law which fulfils the elements of an offence contained in a penal act or an act which permits punishment by non-criminal fine, or if it would constitute such an act also under German law if the facts were transposed to an analogous context, 2. a seizure order issued by a competent authority of the requesting state has been submitted or such an authority has made a declaration stating that the requirements for seizure would be fulfilled if the objects were located in the requesting state, and 3. an assurance is given that the rights of third parties will remain unaffected and that objects surrendered subject to reservation will be returned immediately upon request. (3) The public prosecution office at the Regional Court shall prepare the decision on surrender and carry out surrender once it has been authorised. The public prosecution office at the Regional Court in whose region the objects are located shall have local jurisdiction. Section 61 subsection (2), second sentence, shall apply accordingly. Section 67 Search and seizure (1) Objects that may become the subject of surrender to a foreign state may be seized or

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, <i>ordre public</i> 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,	otherwise secured even prior to the receipt of the request for surrender. A search may also be conducted for this purpose. (2) Subject to the conditions set forth in section 66 subsection (1) number 1 and subsection (2) number 1, objects may also be seized or otherwise secured if necessary for the execution of a request which is not directed toward the surrender of the objects. Subsection (1), second sentence, shall apply accordingly. (3) The search and seizure shall be ordered by the Local Court in whose district the actions are to be conducted. Section 61 subsection (2), second sentence, shall apply accordingly. (4) In case of imminent danger, the public prosecution office and its investigative personnel (section 152 of the Courts Constitution Act) shall be authorised to order the search and seizure.
--	---

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, <i>ordre public</i> or other essential interests.	Article 30 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 (“IRG”) in the absence of applicable international agreements, see Article 25 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.	Article 31 is covered by Sections 66 and 67 of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 (“IRG”) in the absence of applicable international agreements, see Article 29 above.

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.	
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.	German Code of Criminal Procedure (Strafprozessordnung), 2008 (“StPO”): Section 94 Objects Which May Be Seized (1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured. (2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily. (3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.
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	Article 33 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 (“IRG”) in the absence of applicable international agreements, see Article 25 above.

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.	
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.	Article 34 is covered by Sections 59 ff. of the Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 ("IRG") in the absence of applicable international agreements, see Article 25 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 communications with the point of contact of another Party on	Germany has established a 24/7 contact point within the Federal Police Agency (Bundeskriminalamt, "BKA"). It is a member of the 24/7 Network of the "G8 High-Tech Crime Subgroup" and of the ICPO Interpol.

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.	
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.	Declaration contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl. In accordance with Article 40 of the Convention, the Federal Republic of Germany declares that it avails itself of the possibility of requiring that, (a) according to Article 2, second sentence, the additional element of commission by infringing security measures be included as an element of the offence of data espionage, which has been established under German law in section 202a of the Criminal Code pursuant to Article 2, first sentence, and (b) according to Article 7, second sentence, the additional element of an "intent to defraud, or similar dishonest intent" that takes the form of deception in legal transactions be included as an element of the offence of falsification of legally relevant data, which has been established under German law in section 269 of the Criminal Code pursuant to Article 7, first sentence. Reservation contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl. The Federal Republic of Germany declares that it avails itself of Article 42 of the Convention to the extent that (a) Article 6, paragraph 1.a.i, as relates to "devices", and sub-paragraph b shall not be applied,

	(b) the attempt to commit the acts specified under Article 3 shall not be established as criminal offence under national law, and (c) requests for expedited preservation of stored data under Article 29 may be refused on the ground that dual criminality is not given, provided there is reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled, unless the offence in question is an offence established pursuant to Articles 2 to 11. Declaration contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl. In accordance with Article 24, paragraph 7, sub-paragraph a, of the Convention, the Federal Republic of Germany declares that the central authority responsible for making or receiving requests for extradition or provisional arrest is the Federal Foreign Office (address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin). Declaration contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl. In accordance with Article 35, paragraph 1, of the Convention, the Federal Republic of Germany declares that the point of contact designated to fulfil the functions specified in this article is the National High Tech Crime Unit at the Federal Criminal Police Office (address: Thaerstr. 11, 65193 Wiesbaden, phone: 49-611-551-3101, fax: 49-611-554-5100, mail: so43auswertung@bka.bund.de (for non-emergency use only), nhtcu@bka.de (for emergency use only)). Declaration contained in a letter from the Permanent Representative of Germany, dated 14 May 2009, registered at the Secretariat General on 15 May 2009 - Or. Engl. In accordance with Article 27, paragraph 2.a, of the Convention, the Federal Republic of Germany declares that the central authority responsible for mutual assistance requests in the absence of applicable international agreements is the Ministry of Foreign Affairs (address: Werderscher Markt 1, 10117 Berlin)
--	--

