Poland

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 06 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

State:	
Signature of the Budapest Convention:	23/11/2001
Ratification/accession:	20/02/2015

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	**Penal Code** Art. 267. § 1. Anyone who, without being authorised to do so, acquires information not intended for him or her, by opening a sealed letter, or connecting

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information is liable to a fine, the restriction of liberty or imprisonment for up to two years. § 2. Anyone who accesses any part of a computer system without being authorised to do so is liable to the same penalty § 4. Anyone who divulges to another person the information obtained in the manner specified in §§ 1-3 is liable to the same penalty. § 5. The prosecution of the offences specified in §§ 1-4 takes place at the motion of the aggrieved party.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Penal Code** Art 267 § 3. Anyone who installs or uses any audio, visual or other special equipment in order to acquire information to which he or she is not authorised to access, is liable to the same penalty. § 4. Anyone who divulges to another person the information obtained in the manner specified in §§ 1-3 is liable to the same penalty. § 5. The prosecution of the offences specified in §§ 1-4 takes place at the motion of the aggrieved party.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Penal Code** Art. 268. § 1. Anyone who, without being authorised to do so, destroys, damages, deletes or alters a record of essential information, or otherwise prevents or makes it significantly hinders an authorised person from obtaining knowledge of that information, is liable to a fine, the restriction of liberty or imprisonment for up to two years. § 2. If the act specified in § 1 concerns the record on computer storage media, the offender is liable to imprisonment for up to three years. § 3. Anyone who, by committing an act specified in §§ 1 or 2, causes a significant loss of property is liable to imprisonment for between three months and five years. § 4. The prosecution of the offences specified in § 1-3 takes place at the motion of the aggrieved party Art. 268a. § 1. Anyone who, without being authorised to do so, destroys, damages, deletes or alters or hinders access to information data, or who hinders or prevents the automatic collection and transmission of such data is liable to imprisonment for up to three years. § 2. Anyone who, by committing the offence specified in § 1, causes a significant loss of property is liable to imprisonment for between three months and five years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	§ 3. The prosecution of the offences specified in §§ 1-2 takes place at the motion of the aggrieved party.
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	**Penal Code** Art. 269. § 1. Anyone who destroys, deletes or changes a record on computer storage media that is of particular significance for national defence, transport safety, the operation of the government or any other state authority or local government, or that interferes with or prevents the automatic collection and transmission of such information is liable to imprisonment for between six months and eight years. § 2. Anyone who commits the act specified in § 1 by destroying or exchanging a data carrier, or by destroying or damaging a device used for the automatic processing, collection or transmission of information is liable to the same penalty. Art. 269a. Anyone who, without being authorised to do so, by transmitting, damaging, deleting, destroying or altering information data, significantly disrupts a computer system or telecommunications network is liable to imprisonment for three months to five years.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and	**Penal Code** Art. 269b. § 1. Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit the offences specified under Article 165 § 1 section 4, Article 267 § 2, Article 268a § 1 or § 2 in connection with § 1,Article 269 § 2 or Article 269a, including also computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network is liable to imprisonment for up to three years. § 2. In the event of a conviction for the offence specified in § 1, the court orders the forfeiture of the items referred to therein, and may order the forfeiture even if they do not constitute the property of the offender.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	Penal Code Art. 287. § 1. Anyone who, in order to achieve material benefits or to inflict damage upon another person, affects the automatic processing, collection or transmission of data, or changes, deletes or introduces new entries, without being authorised to do so, is liable to imprisonment for between three months and five years. § 2. If the act is of less significance, the offender is liable to a fine, the restriction of liberty or imprisonment for up to one year. § 3. If the offence is committed against a next of kin, the prosecution takes place at the motion of the aggrieved party.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct	**Penal Code** Art. 202. § 3. Anyone who, with the aim of distribution, produces, preserves, imports, stores or possesses, distributes or propagates pornographic material with the participation of a minor, or pornographic material associated with the use of violence or the use of an animal, is liable to imprisonment for between six months and eight years. § 4. Anyone who preserves pornographic material with the participation of a minor under the age of 15 is liable to imprisonment for up to 10 years. § 4a. Anyone who imports, stores or possesses pornographic material with the participation of a minor under the age of 15 is liable to imprisonment for between three months and five years. § 4b. Anyone who produces, distributes, presents, stores or possesses pornographic material presenting a produced or processed image of a minor involved in a sexual act is liable to a fine, the restriction of liberty or imprisonment for up to two years. § 5. The court may decide upon forfeiture of means or other items that were intended to be used or were used to commit offences described in § 1-4b, even if they were not owned by the offender

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Penal Code** Art 278 § 1. Anyone who intentionally steals someone else's movable property is liable to imprisonment for between three months and five years. § 2. Anyone who, without the permission of an authorised person, acquires someone else's computer software with the purpose of gaining a material benefit is liable to the same penalty. § 3. If the act is of less significance, the offender is liable to a fine, the restriction of liberty or imprisonment for up to one year. Art. 293. Receiving stolen software. § 1. The provisions of Articles 291 and 292 apply accordingly to computer software. § 2. The court may decide on the forfeiture of the items specified in § 1 and in Articles 291 and 292, even if it is not the property of the offender. **Act of 4 February 1994 on copyright and related rights** Article 116. 1. Whoever, without authorization or against its terms and conditions, disseminates other persons' work, artistic performance, phonogram, videogram or broadcast in the original or derivative version shall be liable to a fine, restriction of liberty or imprisonment for up to 2 years. 2.If the offender commits the act specified in paragraph 1 above in order to gain material benefits, he/she shall be liable to imprisonment for up to 3 years. 3.If the offender commits the offence specified in paragraph 1 above a regular source of income or organizes or manages a criminal activity as specified in paragraph 1, he/she shall be liable to imprisonment for 6 months to 5 years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	4. If the offender of the act specified in paragraph 1 above acts unintentionally, he/she shall be liable to a fine, restriction of liberty or imprisonment for up to one year. Article 117. 1. Whoever fixes or reproduces other persons' work in its original versions or in the form of derivative version, artistic performance, phonogram, videogram or broadcast for the purposes of its dissemination and gives his/her consent to its dissemination without the authorization or against the conditions specified therein, shall be liable to a fine, restriction of liberty or imprisonment for up to 2 years. 2. If the offender commits the offence specified in paragraph 1 a regular source of income or organizes or manages a criminal activity, as specified in paragraph 1 above, he/she shall be liable toimprisonment for up to 3 years. Article 118. 1. Whoever, in order to gain material benefit purchases, assists in the sale of, accepts or assists in concealing objects being carriers of a piece of work, artistic performance, phonogram, videogram disseminated or reproduced without authorization or against the conditions specified therein, shall be liable to imprisonment for 3 months to 5 years. 2.If the offender committed the crime specified in paragraph 1 above a permanent source of income, or organizes or manages a criminal activity as specified in paragraph 1, he/she shall be liable to imprisonment for up to 5 years. 3.If based on concurrent events the offender of the crime referred to in paragraph 1 or 2 should and might have assumed that an item was received in result of an illicit action, he/she shall be liable to a fine, restriction of liberty or imprisonment for up to 2 years.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
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.	**Data Protection Act** Article 49 (1). A person, who processes personal data in a data filing system where such processing is forbidden or where he/she is not authorised to carry out such processing, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to two years. 2. Where the offence mentioned in point 1 of this article relates to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade union membership, health records, genetic code, addictions or sexual life, the person who processes the data shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to three years. Article 50.1. A person who, being the controller of a data filing system, stores personal data incompatibly with the intended purpose for which the system has been created, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 51.1. A person who, being the controller of a data filing system or being obliged to protect the personal data, discloses them or provides access to unauthorised persons, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to two years. 2. In case of unintentional character of the above offence, the offender shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year. Article 52. A person who, being the controller of a data filing system violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorised takeover, damage or destruction, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year. Article 53. A person who, regardless of the obligation, fails to notify the data filing system for registration, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of up to one year. Article 54. A person who, being the controller, fails to inform the data subject of its rights or to provide him/her with the information which would enable that person to benefit from the provisions of this Act, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of up to one year
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the	**Code of Criminal Procedure** Article 218a § 1 of the CCP: Offices, institutions and entities running their activity in the telecommunication sector shall be obligated, upon the court or public

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	prosecutor demand included in their order, to secure immediately, for a specified period not exceeding 90 days, computer data stored in a equipment that contains this data on a data carrier or computer system (unofficial translation) **Telecommunication Act** Article 180a.1.Subject to Article 180c (2) (2), an operator of a public telecommunications network and a provider of publicly available telecommunications services shall be obliged at their cost to: 1)retain and store data referred to in Article 180c generated in a telecommunications network or processed by that operator or provider, in the territory of the Republic of Poland, for the period of 12 months counted from the day of a call or an unsuccessful call attempt, and to erase the data as of the expiry of this period, excluding data protected under separate provisions. 2)make available the data referred to in point 1 to authorised entities as well as to the court and prosecutor under the terms and procedure specified in separate provisions; 3)protect data referred to in point 1 against accidental or unlawful destruction, loss or alternation, unauthorised or unlawful storage, processing, access or disclosure, in accordance with the provisions of Articles159-175a, Article 175c and Article 180e.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the 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	**Police Act**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	Article 20c. 1. Data that identify a telecommunications network subscriber, termination points of a network or telecommunications device, data about completed or attempted connections between specific telecommunications devices or network termination points, and the circumstances and type of the connection may be disclosed to the Police and processed by the Police only with the view to crime prevention or detection. 2. The data referred to in Paragraph 1 may be disclosed: (1) at a written request of the Police Commander in Chief or a Voivodship Police Commander, (2) verbal request of a police officer being in possession of a written authorisation issued by the persons referred to in Subparagraph 1 above. 3. Telecommunications network operator shall notify disclosure of the data referred to in Paragraph 2 (2) to the territorially competent Voivodship Police Commander. 4. Telecommunications network operators shall disclose the data referred to in Paragraph 1 to the police officers specified in the request lodged by a Police authority. 5. The data referred to in Paragraph 1 may be disclosed via a telecommunications network. 6. The Police shall forward the materials obtained as a result of activities provided for in Paragraph 2 and containing information important for criminal proceedings to the territorially and technically competent prosecutor. 7. Materials obtained as a result of the activities provided for in Paragraph 2 and not containing any information which could be important for criminal proceedings shall be immediately destroyed in the presence of a committee, the fact being officially recorded. 8. The costs of disclosure of the data referred to in Paragraph 1 shall be incurred by the telecommunications network operator. **Telecommunication Act** Article 180c.1.The obligation referred to in Article 180a (1) shall cover the data necessary to: 1)trace the network termination point, telecommunications terminal equipment, an end user: a) originating the call, b) called; 2)identify: a) the date and time of a call and its duration, b) the type of a call, c) location of telecommunications terminal equipment. 2.The Minister competent for digitalization in agreement with the Minister competent for internal affairs, having regard to the type of telecommunications activities performed by operators of a public telecommunications network or providers of publicly available telecommunications services, data specified in paragraph 1, costs of data collection and retention as well as the need to avoid multiple retention and storage of the same data, shall specify, by means of an ordinance: 1)a detailed list of data referred to in paragraph 1;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2)types of public telecommunications network operators or providers of publicly available telecommunications services obliged to retain and store the data. Article 180d.Telecommunications undertakings shall be obliged to provide conditions for access and retention as well as to make available at their own cost the data referred to in Article 159 (1) (1) and (3) to (5), in Article 161 and in Article 179 (9) related to the provided telecommunications service and processed by them to authorized entities, the court and to the prosecutor, under the terms and observing the procedures specified in separate provision **Code of Criminal Procedure** Article 218. § 1. Offices, institutions and entities operating in post and telecommunications fields, customs houses, and transportation institutions and companies, shall be obligated to surrender to the court or state prosecutor upon demand included in their order, any correspondence or transmissions significant to the pending proceedings. Only the court and a state prosecutor shall be entitled to inspect them or to order their inspection. § 2. The announcement of the order referred to in § 1, may be adjourned for a prescribed period, necessary to promote the proper conduct of the case.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:	**Code of Criminal Procedure** Article 219. § 1. A search may be made of premises and other places in order to detect or detain a person or to ensure his compulsory appearance, as well locate objects which might serve as evidence in criminal proceedings, if there is good reason to suppose that the suspected person or the objects sought are to be located there. Article 220. § 1. A search may be conducted by the state prosecutor, or, a with warrant issued by the court or state prosecutor, by the Police, and, also in cases specified in law, by another agency. § 2. The person on whose premises the search is to be conducted should be presented with a warrant issued by a court or state prosecutor. § 3. If the court's or state prosecutor's warrant cannot be issued, Article 217 § 3 shall apply accordingly in cases not amenable to delay. Article 227. Searching or seizing objects shall be conducted in accordance with the objective of the action, with moderation and respect for the dignity of the persons to whom the action relates, and without unnecessary damage or hardship.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Article 236. Orders regarding search and seizure shall be subject to interlocutory appeal by a person whose rights have been violated.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Code of Criminal Procedure** Article 241. The provisions of this chapter shall apply respectively to surveillance and recording by technical means, of the content of information transmissions other than telephone conversations.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 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	

Back to the Table of Contents

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

Back to the Table of Contents

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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
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;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
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 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.	The 24/7 Network point of contact designated by Poland is the: Cybercrime Bureau, National Police Headquarters

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Reservation contained in the instrument of ratification deposited on 20 February 2015** Pursuant to Article 29, paragraph 4, of the Convention, the Republic of Poland reserves that the execution of a request for mutual assistance regarding search or similar access, seizure or similar securing, or disclosure of stored data, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, shall be conditional on dual criminality of those offences.

Back to the Table of Contents