Czech Republic

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State: Czech Republic	
Signature of the Budapest Convention:	9 February 2005
Ratification/accession:	22 August 2013 (entry into force 1 December 2013)

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	"Computer system" and "computer data" are directly applicable from the convention. The term "traffic data" can be found within the Act No. 127/2005 Coll. (Electronic Communications Act), the term "service provider" is defined in the Section 2 lit. d) of the Act No. 480/2004 Coll. (Act on certain information society services).
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	***Czech Criminal Code No. 40/2009 Coll. - Section 230 Subsection 1*** ***Unauthorised Access to Computer System and Information Media*** (1) Whoever overcomes security measures and thus gains access to a computer system or a part thereof without authorisation, shall be sentenced to imprisonment for up to two years, to prohibition of activity, or to forfeiture of things.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	***Section 182(1) lit. c) of the Czech Criminal Code No. 40/2009 Coll. - Breach of Secrecy of Correspondence*** (1) Who intentionally breaches the secret of c) a non-public transfer of computer data to a computer system, out of it or within it, including electromagnetic emissions from a computer system that transfers such computer data, shall be sentenced to imprisonment for up to two years or to prohibition of activity.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	***Section 230 Subsection 2 lit. b) and c) of the of the Czech Criminal Code No. 40/2009 Coll. - Unauthorised Access to Computer System and Information Media*** (2) Whoever gains access to a computer system or information medium and b) erases or otherwise destroys, damages, amends, suppresses, or corrupts the quality of data stored in a computer system or information media, or renders them unusable without authorisation, c) forges or alters data stored in a computer system or information media so as to be considered authentic and according to them it was treated as if it was

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	authentic data, notwithstanding the fact whether the data is directly readable and understandable, or shall be punished by a prison sentence of up to three years, punishment by disqualification, or forfeiture of things.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	***Section 230 Subsection 2 lit. b), c) d) in connection with Section 230 Subsection 3 lit. b) of the Czech Criminal Code No. 40/2009 Coll. - Unauthorised Access to Computer Systems and Information Media*** (2) Whoever gains access to a computer system or information medium and b) erases or otherwise destroys, damages, amends, suppresses, or corrupts the quality of data stored in a computer system or information media, or renders them unusable without authorisation, c) forges or alters data stored in a computer system or information media so as to be considered authentic and according to them it was treated as if it was authentic data, notwithstanding the fact whether the data is directly readable and understandable, or d) inserts data into a computer system or information media or performs any other intervention into the software or hardware of the computer or other technical data processing equipment without authorisation, shall be punished by a prison sentence of up to three years, punishment by disqualification, or forfeiture of things. (3) An offender shall be sentenced to imprisonment for six months to four years, prohibition of activity, or forfeiture of things if he/she commits the act referred to in Subsection (1) or (2) b) with the intention to limit the functionality of a computer system or other technical equipment for data processing without an authorisation.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, 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.	***Czech Criminal Code No. 40/2009 Coll. -*** ***Section 231 Obtaining and Possession of Access Device and Computer System Passwords and other such Data*** (1) Whoever with the intent to commit a criminal offence of Breach of secrecy of correspondence under Section 182(1) b), c) or a criminal offence of Unauthorised access to computer system and information media under Section 230(1), (2) produces, puts into circulation, imports, exports, transits, offers, provides, sells, or otherwise makes available, obtains for him/herself or for another, or handles a) a device or its component, process, instrument or any other means, including a computer programme designed or adapted for unauthorised access to electronic communications networks, computer system or a part thereof, or b) a computer password, access code, data, process or any other similar means by which it is possible to gain access to a computer system or a part thereof, shall be sentenced to imprisonment for up to two years, to forfeirute of things, or to prohibition of activity. (2) An offender shall be sentenced to imprisonment for up to three years, to prohibition of activity, or to forfeiture of things, if he/she a) commits the act referred to in Sub-section (1) as a member of an organised group, or b) gains for him-/herself or for another substantial profit by such an act. (3) An offender shall be sentenced to imprisonment for six months to five years, if he/she gains for him-/herself or for another substantial profit by the act referred to in Sub-section (1).
Title 2 – Computer-related offences	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	***Section 230 Subsection 2 lit. c) of the Czech Criminal Code No. 40/2009 Coll. - Unauthorised Access to Computer Systems and Information Media*** (2) Whoever gains access to a computer system or information medium and c) forges or alters data stored in a computer system or information media so as to be considered authentic, or and according to them was proceeded as if it was it was authentic data, notwithstanding whether the data is directly readable and comprehensible, shall be punished by a prison sentence of up to three years, punishment by disqualification, or forfeiture of things.
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.	The act described in the Article 8 of the Convention is punishable pursuant to Section 230 Subsection 3 lit. a) [in connection with Section 230 Subsection 2 or Section 230 Subsection 3 lit. b)] of the Criminal Code. If the requirements of the Section 230 Subsection 3 are not fulfilled, the criminal liability according to Section 209 in connection with Section 120 of the Criminal Code also comes into account (see below). ***Section 230 Subsection 3 lit. a) of the of the Czech Criminal Code No. 40/2009 Coll. - Unauthorised Access to Computer System and Information Media*** (2) Whoever gains access to a computer system or information medium and a) uses data stored in a computer system or information media without authorisation,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	b) erases or otherwise destroys, damages, amends, suppresses, or corrupts the quality of data stored in a computer system or information media, or renders them unusable without authorisation, c) forges or alters data stored in a computer system or information media so as to be considered authentic and according to them it was treated as if it was authentic data, notwithstanding the fact whether the data is directly readable and understandable, or d) inserts data into a computer system or information media or performs any other intervention into the software or hardware of the computer or other technical data processing equipment without authorisation, shall be punished by a prison sentence of up to three years, punishment by disqualification, or forfeiture of things. (3) An offender shall be sentenced to imprisonment for six months to four years, prohibition of activity, or forfeiture of things if he/she commits the act referred to in paragraph (1) or (2) a) with the intention to cause damage to another person or to obtain an illicit profit for him-/herself or for another, or b) with the intention to limit the functionality of a computer system or other technical equipment for data processing without an authorisation. ***Section 209 (fraud) in connection with Section 120 of the of the Czech Criminal Code No. 40/2009 Coll.*** (1) Whoever enriches him-/herself or another by inducing error in someone, by using someone's error, or by concealing material facts and thus causing damage not insignificant to property of another, shall be sentenced to imprisonment for up to two years, to prohibition of activity, or to forfeiture of a thing.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) An offender shall be sentenced to imprisonment for six months to three years, if he/she commits the act referred to in Sub-section (1) and has been convicted or punished for such an act in the past three years. (3) An offender shall be sentenced to imprisonment for one to five years or to a pecuniary penalty, if he/she causes larger damage by the act referred to in Sub-section (1). (4) An offender shall be sentenced to imprisonment for two to eight years, if he/she a) commits the act referred to in Sub-section (1) as a member of an organised group, b) commits such an act as a person having a particular obligation to defend the interests of the aggrieved person, c) committed such an act in a state of national emergency or a state of war, natural disaster or during another event seriously threatening the life or health of people, public order or property, or d) causes substantial damage by such an act. (5) An offender shall be sentenced to imprisonment for five to ten years, if he/she a) causes extensive damage by the act referred to in Sub-section (1), or b) commits such an act in order to facilitate or enable commission of a terrorist criminal offence, criminal offence of Terrorism financing (Section 312d) or Threat by terrorist criminal offence (Section 312f). (6) Preparation is criminal. ***Section 120 of the Czech Criminal Code - Misleading of Persons and Using their Error by the Means of a Technical Appliance*** Misleading of persons or using their error may be committed also by interfering with computer information or data, interfering with software equipment of a computer or by performing another operation on a computer, interfering with an electronic or other technical appliance, including an interference with objects designated to control such an appliance, or by using such an operation or interference performed by another person.
Title 3 – Content-related offences	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	***Czech Criminal Code No. 40/2009 Coll.*** ***Section 192 Production and other Disposal with Child Pornography*** (1) Whoever handles photographic, film, computer, electronic or other pornographic works, displaying or otherwise using a child or a person that appears to be a child, shall be sentenced to imprisonment for up to two years. (2) Whoever accesses child pornography through information or communication technologies shall be punished accordingly. (3) Whoever produces, imports, exports, transports, offers, makes publicly available, provides, puts into circulation, sells or otherwise procures photographic, film, computer, electronic or other pornographic works that display or otherwise use a child or a person that appears to be a child, or whoever exploits such pornographic works, shall be sentenced to imprisonment for six months to three years, to prohibition of activity or to forfeiture of a thing. (4) An offender shall be sentenced to imprisonment for two to six years or to forfeiture of property, if he/she commits the act referred to in Sub-section (3) a) as a member of an organised group, b) by press, film, radio, television, publicly accessible computer network, or in other similarly effective way, or c) with the intention to gain substantial profit for him-/herself or for another. (4) An offender shall be sentenced to imprisonment for three to eight years or to forfeiture of property, if he/she commits the act referred to in Sub-section (3) a) as a member of an organised group operating in more states, or b) with the intention to gain extensive profit for him-/herself or for another. ***Section 193a Participation in pornographic performance*** Whoever participates in a pornographic or any other similar performance in which a child performs shall be punished by a prison sentence of up to two years. ***Section 126 Child***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	As a child shall be understood a person under 18 years of age, unless the Criminal Code provides otherwise.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	***Section 270 Czech Criminal Code No. 40/2009 Coll.*** ***Infringement of Copyright, Rights Related to Copyright and Rights to Databases*** (1) Whoever wrongfully interferes not insignificantly with legally protected right to an author work, artistic performance, sound or audiovisual record, radio or television broadcast or database, shall be sentenced to imprisonment for up to two years or to prohibition of activity or forfeiture of a thing. (2) An offender shall be sentenced to imprisonment for six months to five years, to a pecuniary penalty or to forfeiture of a thing, if a) the act referred to in Sub-section (1) has attributes of business activity or another enterprising, b) he/she gains for him/herself him-/herself or for another substantial profit or causes substantial damage by such an act, or c) he/she commits such an act in considerable extent. (3) An offender shall be sentenced to imprisonment for three to eight years, if he/she a) gains for him-/herself or for another extensive profit or causes extensive damage to another by the act referred to in Sub-section (1), or b) commits such an act in large extent.
Title 5 – Ancillary liability and sanctions	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	***Sections 21, 23, 24 Czech Criminal Code No. 40/2009 Coll.*** ***Section 21 Attempt*** (1) A conduct imminently leading to completion of a criminal offence, which has been undertaken by the offender with the intent to commit such an offence, shall be considered as an attempt to commit an offence, unless the offence was completed. (2) Attempt to commit an offence shall be punishable according to the term of sentence for the respective completed criminal offence. (3) Criminal liability for an attempted criminal offence shall expire if an offender voluntarily abandoned further conduct leading to the completion of the criminal offence and a) removed the threat to an interest protected by the Criminal Code which occurred due to the committed attempt, or b) reported the attempt to commit an especially serious felony at a time the threat to an interest protected by the Criminal Code which occurred due to the committed attempt could still be removed; the report must be made to a public prosecutor or police authority. A soldier may report it to his/her superior officer. (4) If there are several persons involved in an act, expiration criminal liability for the attempt is not precluded in case of an offender who acted in such manner, if the act is completed by the other offenders despite his/her timely reporting or earlier participation in such an act. (5) The provisions of Sub-section (3) and (4) shall have no effect on the criminal liability of an offender for any other completed criminal offence which they have committed by their conduct referred to in Sub-section (1). ***Section 23 Accomplice*** If a crime is committed by joint intentional conduct of two or more persons, each of them shall be criminally liable as if they alone had committed the offence (accomplices). ***Section 24 Participant*** (1) A participant in a completed offence, or an attempt to commit an offence, is anyone who intentionally

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a) plotted or directed commission of a criminal offence (an organiser); b) instigated another person to commit the criminal offence in (counsel), or c) enabled or facilitated commission of a criminal offence by another person, in particular by providing the means, removing of barriers, eliciting the aggrieved person to the crime scene, keeping watch during commission of an act, providing advice, encouraging the resolve or promising to participate in a criminal offence (aidor). (2) Criminal liability and criminality of an act of a participant shall be governed by provisions on criminal liability of an offender and criminality of an act, unless this Code stipulates otherwise. (3) Criminal liability of the participant shall expire, if he/she voluntarily abandons any further participation in commission of a crime and a) eliminates the threat to an interest protected by this Code arising from his/her participation in the offence; or b) reports his/her attempt at a time when the threat to an interest protected by this Code arising from his/her participation in the offence could still be eliminated. The report must be made to a public prosecutor or police authority. A soldier may report it to his/her superior officer. (4) If there are several persons involved in an act, expiration criminal liability for the participation is not precluded in case of an participant who acted in such manner, if the act is completed by the other offenders despite his/her timely reporting or earlier participation in such an act. (5) The provisions of Sub-section (3) and (4) shall have no effect on the criminal liability of an offender for any other completed criminal offence which they have committed by their conduct referred to in Sub-section (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 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.	***Section 7 and Section 8 of the Act on criminal liability of legal persons and proceedings against them No. 418/2011 Coll.*** ***Section 7*** ***Criminal Acts*** Criminal acts for the purpose of this Act are to be understood as misdemeanours or felonies stipulated in the Criminal Code, with the exception of Manslaughter (Section 141 of the Criminal Code), Murder of a Newborn Child by its Mother (Section 142 of the Criminal Code), Accessory to Suicide (Section 144 of the Criminal Code), Brawling (Section 158 of the Criminal Code), Intercourse among

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Relatives (Section 188 of the Criminal Code), Abandoning a Child or Entrusted Person (Section 195 of the Criminal Code), Negligence of Mandatory Support (Section 196 of the Criminal Code), Maltreatment of a Person Living in Common Residence (Section 199 of the Criminal Code), Breach of Regulations on Rules of Economic Competition (Section 248 (2) of the Criminal Code), High Treason (Section 309 of the Criminal Code), Abusing Representation of State or International Organization (Section 315 of the Criminal Code), Collaboration with Enemy (Section 319 of the Criminal Code), War Treason (Section 320 of the Criminal Code), Service in Foreign Armed Forces (Section 321 of the Criminal Code), Liberation of Prisoners (Section 338 of the Criminal Code), Violent Crossing of State Borders (Section 339 of the Criminal Code), Mutiny of Prisoners (Section 344 of the Criminal Code), Dangerous pursuing (Section 354 of the Criminal Code), Insobriety (Section 360 of the Criminal Code), criminal offenses against conscription stipulated in Chapter XI of the Criminal Code, Military criminal offenses stipulated in Chapter XII of the Criminal Code and Use of Forbidden Means and Methods of Combat (Section 411 of the Criminal Code). ***Section 8*** ***Criminal Liability of a Legal entity*** (1) Criminal act committed by a legal entity is an unlawful act committed in its interest or within its activity, if committed by a) statutory body or member of the statutory body or other person in a leadership position within the legal entity, who is entitled to act on behalf of or for the legal entity, b) a person in a leadership position within the legal entity, who performs managerial or controlling activities, even if they are not a person as mentioned in paragraph a), c) a person with a decisive authority on management of this legal entity, if his/her act was at least one of the conditions leading to a consequence establishing criminal liability of a legal entity, or d) employee or a person with similar status (thereinafter "employee") while fulfilling his/her duties/tasks, even if they are not a person as mentioned in paragraph a) to c),

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	provided that the act can be attributed to the legal entity in accordance with sub-section (2). (2) Commission of a criminal act as specified in Section 7 can be attributed to a legal entity, if committed by a) action of bodies or persons referred to in sub-section (1) a) to c), or b) an employee referred to in sub-section (1) d) on the grounds of a decision, approval or guidance of bodies of the legal entity or persons referred to in sub-section (1) a) to c), or because the bodies of the legal entity or persons referred to in sub-section (1) a) to c) did not take measures required by other legal regulation or that can be justly required, namely that they did not perform obligatory or necessary control (supervision) over the activities of employees or other persons they are superiors to, or they did not take necessary measures to prevent or avert the consequences of the committed criminal act. (3) Criminal liability of a legal entity is not precluded by the fact that a specific natural person who has acted in a way specified in sub-section (1) and (2) cannot be identified. (4) Sub-section (1) and (2) will apply also if a) the activity specified in sub-sections (1) and (2) took place prior to incorporation of the legal entity, b) the legal entity has been incorporated, but the court decided on nullity of the legal entity, c) the legal act establishing authorisation for acting on behalf of the legal entities is invalid or ineffective, or d) the acting natural person is not criminally liable for such criminal act. (5) The legal entity will be relieved of criminal liability according to sub-section (1) to (4) if it made every effort which could be reasonably required of it in order to prevent the commission of the unlawful act by the persons referred to in sub-section (1).
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	Terms of imprisonment for individual criminal offences described above are to be found above in relation to Articles 2 to 10. If legal requirements are fulfilled,

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	following types of penalties (criminal sanctions) may be imposed on natural persons: ***Section 52 of the Czech Criminal Code No. 40/2009 Coll.*** ***Types of Penalties*** (1) The court may impose the following penalties for committed criminal offences a) prison sentence, b) house arrest, c) community service, d) forfeiture of property, e) monetary penalty, f) forfeiture of a thing, g) disqualification, h) prohibition of keeping and breeding animals, i) prohibition of residence, j) prohibition of entry to sporting, cultural and other social events, k) loss of honorary degrees or accolades, l) loss of military rank, m) deportation. (2) Unless defined otherwise under criminal law, punishment by a prison sentence denotes, a) an unconditional prison sentence, b) a conditional conviction to the punishment by prison sentence,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	c) a conditional conviction to the punishment by prison sentence with supervision. (3) The exceptional punishment is a special type of prison sentence (Section 54). In relation to legal persons Section 15 of the **Act on criminal liability of legal persons and proceedings against them No. 418/2011 Coll.** enumerates penalties (criminal sanctions) as well as protective measures which can be imposed on legal persons if legal conditions are fulfilled: **Types of Sentences and Protective Measures** (1) For criminal acts committed by a legal entity, only the following sentences can be imposed a) dissolution of the legal entity, b) confiscation of property, c) monetary penalty, d) forfeiture of a thing, e) prohibition to perform certain activity, f) prohibition to perform public contracts or to participate in public tenders, g) prohibition to receive endowments (grants) and subsidies, h) publication of a judgement. (2) Protective measure of forfeiture of things can be imposed for criminal acts committed by a legal entity. (3) Punishments and protective measures referred to in sub-section (1) and (2) can be imposed to a legal entity separately or concurrently. However, it is not possible to impose a sentence of monetary penalty concurrently to confiscation of property and a sentence of confiscation of things to forfeiture of the same things.
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:	Respective legislative measures and procedures for the purpose of specific criminal investigations or proceedings are described below in sections related to Articles 16 to 21.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	In accordance with Article 15, the use of respective procedures and powers shall be subject to the relevant conditions and restrictions laid down by national law, as well as safeguards against abuse of those powers and procedures, including commitments entered into under the most relevant international human rights instruments. In the Czech legal system, these guarantees are provided by the implementation of relevant obligations arising from international treaties, such as Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (No. 209/1992 Coll.), as well as relevant provisions of constitutional law, such as Article 13 of the Charter of Fundamental Rights and Freedoms.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Establishment, implementation and application of the powers and procedures of respective investigation instruments are subject to conditions and safeguards provided for under domestic law as it is described in sections related to Articles 16 to 21. Supervision over compliance with the legality in pre-trial proceedings shall be conducted by the public prosecutor according to 174 Subsection 1 of the Code of Criminal Procedure No. 141/1961 Coll. There is also a possibility to request for review of actions taken by a police authority and public prosecutor according to Section 157a of the Code of Criminal Procedure. Section 157a Request for Review of Procedure of police Authority and Public Prosecutor (1) The person, against whom are conducted criminal proceedings, and the aggrieved person have the right to ask the public prosecutor to eliminate delays in the proceedings or any defects in the procedure of the police authority at any time during the pre-trial proceedings. This request is not bound by a time limit. The request must be submitted to the public prosecutor immediately and the public prosecutor must handle it immediately. The applicant must be notified of the outcome of the review. (2) The request for eliminating delays in the proceedings or any defects in procedure of the public prosecutor will be handled by a public prosecutor of the immediately superior public prosecutor's office.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.	***Section 7b Subsection 1 of the Code of Criminal Procedure No. 141/1961 Coll.*** (1) If it is necessary to prevent loss, destruction or alteration of data important for criminal proceedings that is stored in a computer system or on an information medium, the person holding the data or having it under control may be ordered to retain the data unaltered for a period of time specified in the order and to adopt

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	necessary measures to prevent disclosure of the information that retention of data has been ordered. (3) An order under sub-section (1) or (2) may be issued by the presiding judge and in pre-trial proceedings by the public prosecutor or the police authority. The police authority must have a prior consent of the public prosecutor to issue such an order; without prior consent, the order may be issued by the police authority only if the prior consent could not be obtained and the matter cannot be delayed. (4) The order referred to in sub-section (1) or (2) must indicate the data to which it relates, the reason for which the data should be retained or for which the access to it should be prevented, and the period for which the data should be retained or for which the access to it should be prevented, which may not be longer than 90 days. The order must contain instructions about the consequences of failure to comply with the order. (5) The authority which issued the order referred to in sub-section (1) or (2) delivers it immediately to the person to whom it is directed. .
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.	***Part V (protection of data, services and electronic communications networks) of the Act on Electronic Communications and on Amendment to Certain Related Acts No. 127/2005 Coll. (Electronic Communications Act)*** is applicable in this context. In accordance with Section 97 Subsection 3 of the Electronic Communications Act, a legal or natural person providing a public communications network or providing a publicly available electronic communications service is obliged to store traffic and location data for a period of 6 months. This legal or natural person, who stores traffic and location data, is obliged to provide it without delay to the law enforcement authorities for the purposes and in compliance with the conditions stipulated by a special legal regulation (Act No. 141/1961 Coll., On Criminal Procedure). In this way, the police may request traffic data both within criminal proceedings on the basis of Section 88a of the Criminal Procedure Code and when

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	monitoring persons and things on the basis of Act No. 273/2008 Coll., On the Police of the Czech Republic. ***Section 88a*** (1) If it is necessary for the purposes of criminal proceedings conducted for a criminal offence, for which the law prescribes a sentence of imprisonment with the upper limit of at least three years, for a criminal offences of Breach of secrecy of correspondence (Section 182 of the Criminal Code), Fraud (Section 209 of the Criminal Code), Unauthorised access to computer systems and information media (Section 230 of the Criminal Code), Obtaining and possession of access device and computer system passwords and other such data (Section 231 of the Criminal Code), Dangerous threatening (Section 353 of the Criminal Code), Dangerous pursuing (Section 354 of the Criminal Code), Spreading of alarming news (Section 357 of the Criminal Code), Incitement to criminal offence (Section 364 of the Criminal Code), Approval of criminal offence (Section 365 of the Criminal Code) or for an intentional criminal offence, prosecution of which is stipulated by an international treaty binding the Czech Republic, to ascertain data on telecommunication traffic that are subject to the telecommunication secrecy or to which applies protection of personal and mediated data and if the followed purpose cannot be achieved otherwise or it its achieving would be substantially more difficult, the presiding judge will order submitting the data to the court in trial proceedings, and in pre-trial proceedings the judge will order their submitting to the public prosecutor or to the Police authority upon a motion of the public prosecutor. The order for ascertaining data on telecommunication traffic must be issued in writing and must be reasoned, including a specific reference to a promulgated international treaty in case the criminal proceedings is being conducted for a criminal offence, prosecution of which is stipulated by this international treaty. If the request concerns a specific user, the order must include his identity, if it is known. (2) The public prosecutor or the Police authority, by whose decision was the case finally and effectively terminated and in trial proceedings the presiding judge of the panel of the court of the first instance will inform the user referred to in sub-section (1), if he is known, after the final and effective termination of the case, about the ordered ascertaining of data on telecommunication traffic. The information contains identification of the court that issued the order for ascertaining of data on telecommunication traffic and data on the period concerned by this order. The information will also contain an advice on the right to file a petition for a review of the legality of the order for ascertaining of data on telecommunication traffic to the Supreme Court within six months from the day of service of this information. The information will be submitted by the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	presiding judge of the panel of the court of the first instance without an undue delay after the final and effective termination of the case. The public prosecutor, by whose decision was the case finally end effectively terminated will submit the information without an undue delay after the expiration of the time limit for reviewing his decision by the Supreme Public Prosecutor according to Section 174a and the Police authority, by whose decision was the case finally and effectively terminated will submit the information without an undue delay after the expiration of the time limit for reviewing his decision by the public prosecutor according to Section 174 (2) e). (3) The information according to sub-section (2) will the presiding judge, the public prosecutor or the Police authority not submit in proceedings on a felony, for which the law stipulates a sentence of imprisonment with the upper limit of at least eight years, committed by an organised criminal group, in proceedings on a criminal offence committed in favour of an organised criminal group, in proceedings on a criminal offence of Participation in organised criminal group (Section 361 of the Criminal Code), in proceedings on the criminal offense of participation on a terrorist group (Section 312a of the Criminal Code), or if more persons took part in commission of the criminal offence and in relation to at least on of them the criminal proceedings was not finally and effectively terminated, or if criminal proceedings is being conducted against the person, to who is the information to be conveyed, or if giving such information could compromise the purpose of this or another criminal proceedings, or if it could lead to endangering of the security of State, or the life, health, rights or freedoms of persons. (4) The order according to sub-section (1) is not necessary, if the user of the telecommunication device concerned by the data on the executed telecommunication traffic gives his consent to submitting the data.
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.	The rules that enable the production of data [Article 18(1)(a)] are provided in ***Section 78 and 79 of the Code of Criminal Procedure No. 141/1961 Coll.*** ***Section 78*** ***Obligation to Handover or Surrender Things*** (1) Anyone who has a thing that may serve for evidentiary purposes in his possession is obliged to present it upon a request to the court, public prosecutor or police authority; if it is necessary to secure the thing for the purposes of due ascertaining of facts important for criminal proceedings, the person is obliged to surrender such thing upon a request to these authorities. Along with the request the person will be advised that if he fails to comply with the request, the thing

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	may be seized from him, as well as about other consequences of the non-compliance (Section 66). The call to handover or surrender a thing may be made by the presiding judge and in pre-trial proceedings by the public prosecutor or police authority. (2) The obligation referred to in sub-section (1) does not apply to documents or other tangible media containing video, audio or data record, the content of which is related to circumstances subject to prohibition of questioning, unless acquittal of the obligation to keep the matter confidential or acquittal of an obligation of silence occurred. (3) Nobody must be forced to handover or surrender a thing that may, in the time the request for its handover or surrender is made, serve as evidence against him or a person close to him; this is without prejudice to provisions on removal of thing, house search, search of other premises and land and personal search. (4) If it is necessary in order to prevent obstruction of confiscation or forfeiture of a thing, the authority involved in criminal proceedings referred to in sub-section (1) will issue an order that the person, to whom the thing was seized, must not transfer the thing or encumber it during the time of seizure. Any legal action contrary to this order will be null and void; the court will consider the nullity even without a petition. The person concerned must be advised thereof. (5) The person, who handed over or surrendered the thing that may serve for evidentiary purposes, will be immediately issued a written confirmation on takeover of such thing or a transcript of the protocol; therein the thing must be described with sufficient accuracy so that it could be identified. (6) The authority involved in criminal proceedings, to which a thing that may serve for evidentiary purposes was surrendered, will take it into their custody. (7) The person, to whom the thing was seized, is entitled to request at any time its return. The authority involved in criminal proceedings referred to in sub-section (1) will decide on such request without an undue delay. If the request was refused, this person may repeat it no sooner than after 30 days following the full force and effect of such decision, unless he states new reasons.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 79 ***Removal of Things from Possession*** (1) If an thing that may serve for evidentiary purposes in criminal proceedings is not handed over or surrendered by the person who has it in his possession, such a thing may be removed from possession upon an order of the presiding judge an in pre-trial proceedings upon an order of the public prosecutor or police authority. The police authority must have a previous consent of the public prosecutor for issuing such an order; without such consent the police authority may issue such consent only if the previous consent cannot be secured an the matter cannot be delayed. (2) If the authority that issued the order does not perform the removal of the thing from possession by itself, it will be performed by the police authority on the basis of the order. (3) Removal of the tangible thing from possession will be witnessed by a non-participating person. (4) Section 78 (4) through (7) will apply accordingly to a thing that was removed from possession. Furthermore, it is possible to use the possibility to request data on the performed telecommunication traffic according to ***Section 88a of the Criminal Procedure Code.*** ***Section 88a*** (1) If it is necessary for the purposes of criminal proceedings conducted for a criminal offence, for which the law prescribes a sentence of imprisonment with the upper limit of at least three years, for a criminal offences of Breach of secrecy of correspondence (Section 182 of the Criminal Code), Fraud (Section 209 of the Criminal Code), Unauthorized access to computer systems and information media (Section 230 of the Criminal Code), Obtaining and possession of access device and computer system passwords and other such data (Section 231 of the Criminal Code), Dangerous threatening (Section 353 of the Criminal Code), Dangerous

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	pursuing (Section 354 of the Criminal Code), Spreading of alarming news (Section 357 of the Criminal Code), Incitement to criminal offence (Section 364 of the Criminal Code), Approval of criminal offence (Section 365 of the Criminal Code) or for an intentional criminal offence, prosecution of which is stipulated by an international treaty binding the Czech Republic, to ascertain data on telecommunication traffic that are subject to the telecommunication secrecy or to which applies protection of personal and mediated data and if the followed purpose cannot be achieved otherwise or it its achieving would be substantially more difficult, the presiding judge will order submitting the data to the court in trial proceedings, and in pre-trial proceedings the judge will order their submitting to the public prosecutor or to the police authority upon a motion of the public prosecutor. The order for ascertaining data on telecommunication traffic must be issued in writing and must be reasoned, including a specific reference to a promulgated international treaty in case the criminal proceedings is being conducted for a criminal offence, prosecution of which is stipulated by this international treaty. If the request concerns a specific user, the order must include his identity, if it is known. (2) The public prosecutor or the police authority, by whose decision was the case finally and effectively terminated and in trial proceedings the presiding judge of the panel of the court of the first instance will inform the user referred to in sub-section (1), if he is known, after the final and effective termination of the case, about the ordered ascertaining of data on telecommunication traffic. The information contains identification of the court that issued the order for ascertaining of data on telecommunication traffic and data on the period concerned by this order. The information will also contain an advice on the right to file a petition for a review of the legality of the order for ascertaining of data on telecommunication traffic to the Supreme Court within six months from the day of service of this information. The information will be submitted by the presiding judge of the panel of the court of the first instance without an undue delay after the final and effective termination of the case. The public prosecutor, by whose decision was the case finally end effectively terminated will submit the information without an undue delay after the expiration of the time limit for reviewing his decision by the Supreme Public Prosecutor according to Section 174a and the police authority, by whose decision was the case finally and effectively terminated will submit the information without an undue delay after

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the expiration of the time limit for reviewing his decision by the public prosecutor according to Section 174 (2) e). (3) The information according to sub-section (2) will the presiding judge, the public prosecutor or the police authority not submit in proceedings on a felony, for which the law stipulates a sentence of imprisonment with the upper limit of at least eight years, committed by an organized criminal group, in proceedings on a criminal offence committed in favor of an organized criminal group, in proceedings on a criminal offence of Participation in organized criminal group (Section 361 of the Criminal Code), in proceedings on the criminal offense of participation on a terrorist group (Section 312a of the Criminal Code) or if more persons took part in commission of the criminal offence and in relation to at least one of them the criminal proceedings was not finally and effectively terminated, or if criminal proceedings is being conducted against the person, to who is the information to be conveyed, or if giving such information could compromise the purpose of this or another criminal proceedings, or if it could lead to endangering of the security of State, or the life, health, rights or freedoms of persons. (4) The order according to sub-section (1) is not necessary, if the user of the telecommunication device concerned by the data on the executed telecommunication traffic gives his consent to submitting the data. The production of subscriber data by service providers [Article 18(1)(b)] is to be found in Section 66 of the Act No. 273/2008 Coll., on the Police of the Czech Republic. According to this provision Police is entitled to require traffic and location data if legal requiremets are fulfilled.
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.	***Sections 82 - 85(b) of the Code of Criminal Procedure No. 141/1961 Coll.*** ***Section 82*** ***Reasons for House and Personal Search and Search of Other Premises and Parcels***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures 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.	(1) House search may be performed only if there is a reasonable suspicion that in an apartment or in other premises serving as a residence or in appertaining premises (house) is an thing or a person essential for criminal proceedings. (2) For reasons referred to in sub-section (1) may be performed a search of premises not serving as residence (other premises) and parcels, if they are not publicly accessible. (3) Personal search may be performed, if there is a reasonable suspicion that somebody has an thing essential for criminal proceedings on him. (4) Personal search of an apprehended person or a person who is being taken to custody may be performed also if there is a suspicion that he has a weapon or another object that could endanger his life or health, or life or health of other persons. ***Section 83*** ***House Search Warrant*** (1) The presiding judge and in pre-trial proceedings the judge upon a motion of the public prosecutor is entitled to order a house search. In urgent cases may a house search be ordered, instead of the competent presiding judge or judge (Section 18), by the presiding judge or judge, in whose jurisdiction is the house search to be performed. The order for a house search will be issued in writing and will include a justification. The order will be served to the person whose residence is to be searched when the search is commenced, or if that is not possible, within 24 hours from the time the obstacle impeding the service disappeared at the latest. (2) Upon an order of the presiding judge or judge will the house search be performed by the police authority. ***Section 83a*** ***Order for Search of Other Premises and Parcels*** (1) Section 83 (1) and (2) will apply accordingly to proceedings on performing a search of other premises and parcels.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) Without an order may the police authority perform a search of other premises or parcels only if the order cannot be obtained in advance and in the matter cannot be delayed. However, the police authority is obliged to immediately request a consent of the authority competent for issuing the order; in pre-trial proceedings it will be done through the public prosecutor. If the competent authority does not grant the subsequent consent, the outcome of the search cannot be use in further proceedings as evidence. (3) Without the order may the police authority perform a search of other premises or parcels also if the user of the concerned premises or parcels declares in writing that he consents with the search and hands this declaration to the police authority. The police authority must immediately notify such action to the presiding judge entitled to issue the order, and in pre-trial proceedings to the public prosecutor. ***Section 83b*** ***Order for Personal Search*** (1) The presiding judge and in pre-trial proceedings the public prosecutor or with his consent the police authority is entitled to order a personal search. (2) If the personal search is not performed by the authority that ordered it, it will be performed upon its order by the police authority. (3) Personal search will always be performed by a person of the same sex. (4) Without the order or consent referred to in sub-section (1) may the police authority perform a personal search only if the order or consent could not be obtained in advance and the matter cannot be delayed, or if the search concerns a person caught in commission of a crime or a person for whom was issued an arrest warrant. Without an order or consent may a personal search be performed also in cases referred to in Section 82 (4). ***Section 83c*** ***Entering Residences, other Premises and Parcels***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) The police authority may enter a residence, other premises or parcels only if the matter cannot be delayed and the entering these premises is necessary for protection of life or health of persons or for protection of other rights and liberties or for averting a serious threat to public security and order. (2) Furthermore, the police authority is authorized to enter premises referred to in sub-section (1) also if there is a person for whom was issued an arrest warrant, apprehension order or an order to be delivered for execution of a sentence of imprisonment, or to execution of a protective measure associated with incarceration, who needs to be compelled to appear before a court for the purposes of criminal prosecution, or who is required to be apprehended. (3) After entering the abovementioned premises, no other steps can be performed than steps facilitating disposal of an urgent threat or compelling a person to appear before a court. ***Section 84*** ***Previous Questioning*** Performing a house search, a personal search or a search of other premises and parcels is possible only after a previous questioning of the person, in whose premises or on whom is the search to be performed, and only in the event the questioning did not lead to a voluntary surrender of the searched item or elimination of another reason that has led to this action. Previous questioning is not required if the matter cannot be delayed and the questioning cannot be performed immediately. ***Section 85*** ***Enforcement of Searches and Entries into Residences, Other Premises and Land*** (1) The authority performing a house search or a search of other premises is obliged to allow the person, whose premises are searched, or an adult member of his household, or in case of a search of other premises also his employee, to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	participate in the search. This authority is obliged to instruct these persons will about the right to participate in the search. (2) It is also necessary to include a person that is not involved in the matter. The authority performing the search will prove its entitlement. (3) The protocol on the search will also state whether provisions on previous questioning were complied with, eventually it will indicate reasons, for which they were not complied with. In case that during the search has occurred a surrender or removal of an item, it is necessary to include data referred in Section 78 (5) in the protocol. (4) The person, whose premises were searched, will immediately, and if it is not possible, then within next 24 hours, receive a written confirmation of the outcomes of the search from the authority conducting the search, as well as a receipt of taking over things that were surrendered or removed during the search, or a copy of the protocol. (5) Sub-sections (1) to (4) will be applied for entering residences, other premises and parcels accordingly. Participation of persons referred to in sub-section (1) in entering residences may be denied and the person referred to in sub-section (2) may not be included, if their life or health could be imperiled. ***Section 85a*** (1) A person who is to be subject to a house search, search of other premises and parcels, personal search or to an entry to residence, is obligated to tolerate such an action. (2) If a person who is to be subject to an action referred to in sub-section (1) does not enable the performance of such an action, the authorities performing the action are entitled to overcome the resistance of such person or the obstacles they create after previous futile bidding. This fact will be recorded in the protocol (Section 85 (3)).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 85b (1) When conducting a house search or search of other premises in which an attorney practices law, if there may be documents that contain facts which are subject to the obligation of confidentiality of the attorney, the authority performing the action must seek the cooperation of the Czech Bar Association1 (hereinafter referred to as the "Chamber"); the authority performing the action is entitled to peruse the contents of these documents only in the presence and with the consent of a representative Chamber, who is appointed by the President of the Chamber from its employees or from attorneys. The opinion of the Chamber representative is to be noted in the protocol pursuant to Section 85 (3). (2) If the Chamber representative refuses to grant the approval according to sub-section (1), the documents must be secured in the presence of the authority performing the action, an attorney and a Chamber representative, so that their contents cannot be perused by anyone, destroyed or damaged; immediately after that the documents in question must be handed to the Chamber. The Chamber will return those documents to the attorney immediately after the time limit pursuant to sub-section (5) for filing a request expires. The Chamber will proceed similarly, if the petition is dismissed, even in relation to only some of the documents; in this case the Chamber will return only such documents to the attorney, which the dismissal of the request concerns. The Chamber will also return the documents to the attorney immediately after it was informed about the procedure pursuant sub-section (6). (3) In the case referred to in sub-section (2), first sentence, the consent of the Chamber representative may be replaced upon the petition of the authority that ordered the house search or search of other premises based on the decision of the judge of the closest superior court, where operates the presiding judge or judge, who is entitled to order the house search or search of other premises pursuant to Section 83 (1) and Section 83a (1). In case of a house search or search of other premises performed by a police authority according to Section 83a (2) or (3) will the petition according to the first sentence be filed by the presiding judge entitled to issue the order and in pre-trial proceedings the public prosecutor.

[1] Also called the Chamber of Advocates

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) The petition must include, in addition to general requirements (Section 59 (4)), also indication of the documents, in relation to which the petitioner seeks the replacement of the approval of the Chamber representative for the purpose of perusing their contents, and depicting the facts showing why the disapproval of the Chamber representative for the peruse of the contents of such documents should be replaced by the decision of a judge pursuant to sub-section (3). A protocol must be attached to the petition, where the disapproval of the Chamber representative is recorded, so that the authority performing the action may peruse the contents of the documents. (5) The petition must be submitted within 15 days from the day the Chamber representative refused to grant the consent to peruse the documents, in respect of which the petitioner seeks the replacement of the consent of the Chamber representative to peruse the documents pursuant to sub-section (4). (6) A petition that does not contain all the particulars, or which is incomprehensible or vague, will be disregarded by the judge; the provisions of Section 59 (4), sentence three and four, will not apply. The judge will proceed similarly if the petition was filed late or if it was submitted by someone who is not entitled to it. The judge will inform the petitioner and the Chamber on this procedure without undue delay. (7) If the judge does not proceed in accordance with sub-section 6, he will discuss the petition without undue delay in a public session and will order the Chamber to present the documents, regarding which the petitioner seeks replacement of the consent of the Chamber representative to peruse their contents. Among other actions, the judge will also verify, whether the security of the documents submitted by the Chamber has not been breached and will peruse their contents; at the same time he will take measures to ensure that the petitioner or anyone else is not able see the contents of the documents in the public session. (8) If the public session is adjourned, the judge will secure the documents so that no one can peruse their contents, or destroy or damage them. (9) The judge will grant the petition, if he comes to the conclusion that the documents do not contain facts which the attorney in question is obliged to keep confidential; otherwise they will dismiss the petition.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(10) If the judge grants the petition at least in part, he will pass the documents, in relation to which the approval of the Chamber representative to peruse their content was replaced, to the authority performing the action immediately after the full force and effect of the decision, and order it to return the document back to the Chamber as soon as it perused their contents; this does not apply if such documents are to be used as evidence in criminal proceedings. The judge will return the documents, regarding which was the petition dismissed, to the Chamber immediately after the full force and effect of the decision. (11) In the event the documents cannot be handed over to the authority performing the action, to the Chamber, or to their representatives personally, then they will be delivered to them on the next working day following the date on which the decision came into full force and effect, to the authority performing the action, or the Chamber through the judicial process server or a judicial guard. (12) The document referred to in sub-section (1) through (11) will be understood as a written document or its part, as well as other information media.
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	***Section 88 and 88a of the Code of Criminal Procedure No. 141/1961 Coll.*** ***Section 88*** ***Interception and Recording of Telecommunication*** (1) If a criminal proceeding is conducted for a crime, for which the law prescribes a sentence of imprisonment with the upper limit of at least eight years, for a criminal offence of machinations in insolvency proceedings according to Section 226 of the Criminal Code, breach of regulations on rules of economic competition according to Section 248 (1) (e) and (2) to (4) of the Criminal Code, arranging advantage in commission of public contract, public contest and public auction according to Section 256 of the Criminal Code, machinations in commission of public contract and public contest according to Section 257 of the Criminal Code, machinations in public auction according to Section 258 of the Criminal Code, abuse of competence of a public official according to Section 329 of the Criminal Code, false accusation according to Section 345 (3) to (5) of the Criminal Code, perjury according to Section 346 (3) to (5) of the Criminal Code, false translation according to Section 347 (3) to (5) of the Criminal Code or for another intentional

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	criminal offence, for prosecution of which is the Czech Republic bound by a promulgated international treaty, an order for intercepting and recording telecommunication traffic may be issued, if there is a reasonable belief that it will transmit information essential for criminal proceedings and the pursued purpose cannot be achieved in other ways, or if reaching this purpose would otherwise be considerably more complicated. Intercepting and recording of telecommunication traffic for the needs of all authorities involved in criminal proceedings will be performed by the police of the Czech Republic. Intercepting and recording of telecommunication traffic between an accused person and his defense counsel is inadmissible. If the police authority ascertains, in the course of intercepting and recording of telecommunication traffic, that the accused person communicates with his defense counsel, it is obliged to immediately destroy the record and not to use thus ascertained information in any way. Protocol on destroying the record will be deposited in the file (2) Only the presiding judge and in pre-trial proceedings the judge upon a motion of the public prosecutor is entitled to order interception and recording of telecommunication traffic. The order to intercept and record telecommunication traffic must be issued in writing and must be justified, including a specific reference to a promulgated international treaty, if the criminal proceeding is conducted for a criminal offence, to prosecution of which is the Czech Republic bound by this international treaty. The order for interception and recording of telecommunication traffic will indicate the user address or the device and the user himself, if his identity is known, and the time for which is the interception and recording to be conducted, which will not exceed four months; the reasoning must state specific matters of fact that justify the issue of this order, including the time of its duration. The order for interception and recording of telecommunication traffic will be immediately delivered to the police authority. In pre-trial proceedings will a transcript of the order for intercepting and recording of telecommunication traffic be immediately sent to the public prosecutor. (3) The police authority is obliged to continuously assess, whether the reasons that lead to issuing the order for interception and recording of telecommunication traffic still exist. If the reasons ceased to exist, the police authority is obliged to terminate the interception and recording of telecommunication traffic at once, even before the expiration of the time referred to in sub-section (2). This matter will be immediately notified in writing to the presiding judge that issued the order for intercepting and recording of telecommunication traffic, and in pre-trial proceedings also to the public prosecutor and judge.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) Based on evaluation of previous course of interception and recording of telecommunication traffic may the judge of a court of a higher instance and in pre-trial proceedings the judge of a Regional Court upon a motion of the public prosecutor extend the duration of the interception and recording of telecommunication traffic; the extension may be ordered repeatedly, each time for four months at the longest. (5) Without an order for interception and recording of telecommunication traffic may the authority involved in criminal proceedings order interception and recording of telecommunication traffic or perform it by itself, if the matter concerns criminal proceedings conducted for a criminal offence of trafficking in human beings (Section 168 of the Criminal Code), placing a child in custody of another person (Section 169 of the Criminal Code), illegal restraint (Section 171 of the Criminal Code), extortion (Section 175 of the Criminal Code), kidnapping of a child or a mentally challenged person (Section 200 of the Criminal Code), violence against a group of people and against an individual (Section 352 of the Criminal Code), dangerous threatening (Section 353 of the Criminal Code), or dangerous pursuit (Section 354 of the Criminal Code) provided that the user of the intercepted station consents with it. (6) If a record of telecommunication traffic is to be used as evidence, it must be provided with a protocol stating data on the location, time, means and contents of the record, and also information on the authority that made the record. The police authority is obliged to mark and reliably store other records, so that their protection from unauthorized use is secured, and to indicate in the protocol attached to the file where they are stored. In another criminal case than the case in which the interception and recording of telecommunication traffic was performed may the records be used as evidence only if in this case is the criminal prosecution conducted for a criminal offence referred to in sub-section (1), or if the user of the intercepted station consents with it. (7) If no matters substantial for criminal proceedings are ascertained during the interception and recording of telecommunication traffic, the police authority is obliged, upon receiving a consent of the court and in pre-trial proceedings of the public prosecutor, to immediately destroy the records after three years from the final and effective conclusion of the case. If the police authority was notified about filing an extraordinary appeal in the stated time limit, it will destroy the records after the decision on the extraordinary appeal is made, eventually after the new final and effective conclusion of the case. Protocol on destroying the record of the interception will the police authority send to the public prosecutor, by whose decision was the case finally and effectively concluded, and in trial proceedings to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the presiding judge of the court panel of the first instance, in order to be stored in the file. (8) The public prosecutor or police authority, by whose decision was the case finally and effectively concluded, and in trial proceedings the presiding judge of the court panel of the court of the first instance after final and effective conclusion of the case, will inform the person referred to in sub-section (2) about the ordered interception and recording of telecommunication traffic, if this person is known. The information will contain identification of the court that issued the order for interception and recording of telecommunication traffic, duration of the interception and the date of its termination. A part of the information is an instruction about the right to file a petition to the Supreme Court to review the legality of the order for interception and recording of telecommunication traffic within six months from the day of delivering this information. The presiding judge of the court of first instance will give the information immediately after concluding the case, the public prosecutor by whose decision was the case effectively concluded immediately after expiration of the time period for review of his decision by the Supreme Public Prosecutor according to Section 174a, and the police authority, by whose decision was the case finally and effectively concluded, immediately after expiration of the time period for review of its decision by the public prosecutor according to Section 174 (2) e). (9) The information according to sub-section (8) will the presiding judge, public prosecutor or police authority not give in proceedings on a crime, for which the law prescribes a sentence of imprisonment with the upper limit of at least eight years, committed by an organized group, in proceedings on a criminal offence committed for the benefit of an organized criminal group, in proceedings on a criminal offence of participation in an organized criminal group (Section 361 of the Criminal Code), in proceedings on the criminal offense of participation on a terrorist group (Section 312a of the Criminal Code) or if more persons participated in commission of the criminal offence and in relation to at least one of them was the criminal proceedings not yet finally and effectively concluded, or if a criminal proceeding is conducted against the person, to whom is the information to be given, or if giving such information could thwart the purpose of the criminal proceedings, including the proceedings referred to in sub-section (6), or if it could imperil the security of State, life, health or rights and liberties of persons.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 88a (1) If it is necessary for the purposes of criminal proceedings conducted for a criminal offence, for which the law prescribes a sentence of imprisonment with the upper limit of at least three years, for a criminal offences of Breach of secrecy of correspondence (Section 182 of the Criminal Code), Fraud (Section 209 of the Criminal Code), Unauthorized access to computer systems and information media (Section 230 of the Criminal Code), Obtaining and possession of access device and computer system passwords and other such data (Section 231 of the Criminal Code), Dangerous threatening (Section 353 of the Criminal Code), Dangerous pursuing (Section 354 of the Criminal Code), Spreading of alarming news (Section 357 of the Criminal Code), Incitement to criminal offence (Section 364 of the Criminal Code), Approval of criminal offence (Section 365 of the Criminal Code) or for an intentional criminal offence, prosecution of which is stipulated by an international treaty binding the Czech Republic, to ascertain data on telecommunication traffic that are subject to the telecommunication secrecy or to which applies protection of personal and mediated data and if the followed purpose cannot be achieved otherwise or it its achieving would be substantially more difficult, the presiding judge will order submitting the data to the court in trial proceedings, and in pre-trial proceedings the judge will order their submitting to the public prosecutor or to the police authority upon a motion of the public prosecutor. The order for ascertaining data on telecommunication traffic must be issued in writing and must be reasoned, including a specific reference to a promulgated international treaty in case the criminal proceedings is being conducted for a criminal offence, prosecution of which is stipulated by this international treaty. If the request concerns a specific user, the order must include his identity, if it is known. (2) The public prosecutor or the police authority, by whose decision was the case finally and effectively terminated and in trial proceedings the presiding judge of the panel of the court of the first instance will inform the user referred to in sub-section (1), if he is known, after the final and effective termination of the case, about the ordered ascertaining of data on telecommunication traffic. The information contains identification of the court that issued the order for ascertaining of data on telecommunication traffic and data on the period concerned by this order. The information will also contain an advice on the right to file a petition for a review of the legality of the order for ascertaining of data on telecommunication traffic to the Supreme Court within six months from the day of service of this information. The information will be submitted by the presiding judge of the panel of the court of the first instance without an undue

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	delay after the final and effective termination of the case. The public prosecutor, by whose decision was the case finally end effectively terminated will submit the information without an undue delay after the expiration of the time limit for reviewing his decision by the Supreme Public Prosecutor according to Section 174a and the police authority, by whose decision was the case finally and effectively terminated will submit the information without an undue delay after the expiration of the time limit for reviewing his decision by the public prosecutor according to Section 174 (2) e). (3) The information according to sub-section (2) will the presiding judge, the public prosecutor or the police authority not submit in proceedings on a felony, for which the law stipulates a sentence of imprisonment with the upper limit of at least eight years, committed by an organized criminal group, in proceedings on a criminal offence committed in favor of an organized criminal group, in proceedings on a criminal offence of Participation in organized criminal group (Section 361 of the Criminal Code), in proceedings on the criminal offense of participation on a terrorist group (Section 312a of the Criminal Code) or if more persons took part in commission of the criminal offence and in relation to at least one of them the criminal proceedings was not finally and effectively terminated, or if criminal proceedings is being conducted against the person, to who is the information to be conveyed, or if giving such information could compromise the purpose of this or another criminal proceedings, or if it could lead to endangering of the security of State, or the life, health, rights or freedoms of persons. (4) The order according to sub-section (1) is not necessary, if the user of the telecommunication device concerned by the data on the executed telecommunication traffic gives his consent to submitting the data. ***Section 158d of the Code of Criminal Procedure No. 141/1961 Coll. -*** ***Surveillance of Persons and Things*** (1) Surveillance of persons and things (hereinafter referred to as "surveillance") will be understood as acquiring knowledge on persons and things conducted in a classified manner by technical or other means. If a Police authority ascertains that the accused person is communicating with his defence counsel, it is obliged to destroy the record containing this communication and not to use facts learned in this connection in any way. (2) Surveillance, during which will any audio, visual or other records be made, may be performed solely on the basis of a written authorization of a public prosecutor.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) If the surveillance should interfere with inviolability of residence, inviolability of letters or if it should investigate the contents of other documents and records kept in privacy by use of technical means, it can be performed solely on the basis of a prior authorization of a judge. When entering residences, only steps related to placement of technical devices may be made. (4) Authorization according sub-sections (2) and (3) may be issued only upon a written request. The request must be reasoned by a suspicion of a specific criminal activity and if known, also by data on persons or things that are to be monitored. The authorization will state a time limit, for which will the surveillance be conducted and that cannot exceed six months. The authority that authorized the surveillance may prolong the time limit by a written order issued on the basis of a new written request, always for a time limit not exceeding six months. (5) If the matter cannot be delayed and if cases referred to in sub-section (3) are not concerned, the surveillance may be initiated even without an authorization. However, the Police authority is obliged to immediately request the authorization, and if it is not granted within 48 hours, it is obliged to terminate the surveillance, destroy any eventual records and not to use information so ascertained in any way. (6) Without fulfilling the conditions according to sub-sections (2) and (3) may the surveillance be conducted if the person, whose rights and liberties are to be interfered with, grants his explicit consent therewith. If this consent is post facto withdrawn, the surveillance will be immediately terminated. (7) If a record made in the course of surveillance should be used as evidence, it will be accompanied by a protocol with requirements referred to in Sections 55 and 55a. (8) If no matters of fact substantial for criminal proceedings are ascertained during the surveillance, it is necessary to destroy records thereof in a prescribed way. (9) Telecommunication operators, whose employees and other persons participant in operating telecommunication services, as well as postal service or a person conducting transportation of consignments are obliged to cooperate in a necessary extent with the Police authority conducting the surveillance, according to its instructions and free of charge. Therein they cannot invoke their obligation of silence provided for by special laws. (10) In another criminal case than the case in which a surveillance was authorized under conditions referred to in sub-section (2), may the records made in course

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	of the surveillance and attached protocol be used as evidence only if a proceeding for intentional criminal activity is conducted in this case or if the person, whose rights and liberties were interfered with, consents with it.
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.	The rules on interception of data are enshrined in ***Code of Criminal Procedure in the Section 158d*** ***Surveillance of Persons and Things*** (1) Surveillance of persons and things (hereinafter referred to as "surveillance") will be understood as acquiring knowledge on persons and things conducted in a classified manner by technical or other means. If a Police authority ascertains that the accused person is communicating with his defence counsel, it is obliged to destroy the record containing this communication and not to use facts learned in this connection in any way. (2) Surveillance, during which will any audio, visual or other records be made, may be performed solely on the basis of a written authorization of a public prosecutor. (3) If the surveillance should interfere with inviolability of residence, inviolability of letters or if it should investigate the contents of other documents and records kept in privacy by use of technical means, it can be performed solely on the basis of a prior authorization of a judge. When entering residences, only steps related to placement of technical devices may be made. (4) Authorization according sub-sections (2) and (3) may be issued only upon a written request. The request must be reasoned by a suspicion of a specific criminal activity and if known, also by data on persons or things that are to be monitored. The authorization will state a time limit, for which will the surveillance be conducted and that cannot exceed six months. The authority that authorized the surveillance may prolong the time limit by a written order issued on the basis of a new written request, always for a time limit not exceeding six months. (5) If the matter cannot be delayed and if cases referred to in sub-section (3) are not concerned, the surveillance may be initiated even without an authorization. However, the Police authority is obliged to immediately request the authorization, and if it is not granted within 48 hours, it is obliged to terminate the surveillance, destroy any eventual records and not to use information so ascertained in any way.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) Without fulfilling the conditions according to sub-sections (2) and (3) may the surveillance be conducted if the person, whose rights and liberties are to be interfered with, grants his explicit consent therewith. If this consent is post facto withdrawn, the surveillance will be immediately terminated. (7) If a record made in the course of surveillance should be used as evidence, it will be accompanied by a protocol with requirements referred to in Sections 55 and 55a. (8) If no matters of fact substantial for criminal proceedings are ascertained during the surveillance, it is necessary to destroy records thereof in a prescribed way. (9) Telecommunication operators, whose employees and other persons participant in operating telecommunication services, as well as postal service or a person conducting transportation of consignments are obliged to cooperate in a necessary extent with the Police authority conducting the surveillance, according to its instructions and free of charge. Therein they cannot invoke their obligation of silence provided for by special laws. (10) In another criminal case than the case in which a surveillance was authorized under conditions referred to in sub-section (2), may the records made in course of the surveillance and attached protocol be used as evidence only if a proceeding for intentional criminal activity is conducted in this case or if the person, whose rights and liberties were interfered with, consents with it.
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.	***Sections 4 – 9 of the Czech Criminal Code No. 40/2009 Coll.*** ***Section 4*** ***Principle of Territoriality*** (1) The criminality of an act committed in the territory of the Czech Republic will be assessed pursuant to the law of the Czech Republic.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) A criminal offense will be considered as committed in the territory of the Czech Republic a) if an offender committed the act here, either entirely or in part, even though the violation or endangering of an interest protected by the criminal law occurred or was supposed to occur, either entirely or in part abroad, or b) if an offender violated or endangered an interest protected by criminal law or if such a consequence was supposed to occur, even partially, within the territory, even though the act was committed abroad. (3) Participation is committed in the territory of the Czech Republic, a) the act of the offender has been committed within its territory; which is determined analogically according to sub-section (2), or b) if the accomplice of the act committed abroad partially acted within its territory. (4) If the accomplice acted in the territory of the Czech Republic, the law of the Czech Republic will apply to the participation, regardless of whether the act of the offender is criminal abroad. ***Section 5*** ***Principle of Registration*** The criminality of an act committed outside of the territory of the Czech Republic, aboard a ship or another vessel, aircraft or other means of air transport, which is registered in the Czech Republic, will also be assessed in accordance to the law of the Czech Republic. The place of commission of such an act will be assessed according to Section 4 (2) and (3). ***Section 6*** ***Principle of Personality*** The law of the Czech Republic will also apply to assessment of criminality of an act committed abroad by a citizen of the Czech Republic or a person with no nationality, who has been granted a permanent residence in its territory.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 7 ***Principle of Protection and Principle of Universality*** (1) The law of the Czech Republic will apply to assessment of criminality of Torture and other cruel and inhumane treatment (Section 149), Forgery and alteration of money (Section 233), Uttering forged and altered money (Section 235), Manufacture and possession of forgery equipment (Section 236), Unauthorized production of money (Section 237), Subversion of the Republic (Section 310), Terrorist attack (Section 311), Terror (Section 312), Participation in a terrorist group (Section 312a), Terrorism financing (Section 312d), Support and promotion terrorism (Section 312e), Threat by terrorist criminal act (Section 312f), Sabotage (Section 314), Espionage (Section 316), Violence against public authority (Section 323), Violence against a public official (Section 325), Forgery and alteration of public documents (Section 348), Genocide (Section 400), Attack against humanity (Section 401), Apartheid and discrimination against groups of people (Section 402), Preparation of offensive war (Section 406), Use of prohibited means and methods of combat (Section 411), War cruelty (Section 412), Persecution of population (Section 413), Pillage in the area of military operations (Section 414), Abuse of internationally and state recognized symbols (Section 415), Abuse of flag and armistice (Section 416) and Harming a conciliator (Section 417), even when such a criminal offense was committed abroad by a foreign national or a person with no nationality, who has not been granted permanent residence in the territory of the Czech Republic. (2) The law of the Czech Republic will also apply to assessment of criminality of an act committed abroad against a Czech national or a person without a nationality, who has been granted permanent residence in the territory of the Czech Republic, if the act is criminal in the place of its commission, or if the place of its commission is not subject to any criminal jurisdiction. ***Section 8*** ***Subsidiary Principle of Universality*** (1) The law of the Czech Republic will also apply to assessment of criminality of an act committed abroad by a foreign national or a person with no nationality, who has not been granted permanent residence in the territory of the Czech Republic, if

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a) the act is criminal also under the law effective in the territory of its commission, b) the offender was apprehended in the territory of the Czech Republic, the extradition or surrender proceedings took place and the offender was not extradited or surrendered to another state or to another entitled authority for criminal prosecution or execution of a sentence, and c) the foreign state or another entitled entity that requested the surrender or extradition of the offender for criminal prosecution or execution of a sentence has requested that the criminal prosecution of the offender was conducted in the Czech Republic. (2) The law of the Czech Republic will apply to assessment of criminality of an act committed abroad by a foreign national or a person without a nationality to who has not been granted permanent residence in the territory of the Czech Republic, also when the act was committed in favor of a legal entity with a registered office or branch in the territory of the Czech Republic. (3) However, the offender cannot be imposed a more severe sentence than the sentence prescribed by the law of the state, in the territory of which was the criminal offense committed. ***Section 9*** ***Jurisdiction Stipulated by International Treaty*** (1) Criminality of an act will be assessed according to the law of the Czech Republic also if an international treaty incorporated into the system of law (hereinafter referred to as "international treaty") stipulates so. (2) The provisions of Section 4 to 8 will not apply if it is not admissible according to an international treaty.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	***Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended (in particular Section 78 et sequentia)*** ***Article 10 of the Constitution of the Czech Republic*** Promulgated international treaties, the ratification of which has been approved by the Parliament and which are binding upon the Czech Republic, shall constitute a part of the legal order; should an international treaty stipulate anything else than a law, the international treaty shall be applied. Procedure according to Act 104/2013 Coll. will apply, unless an international treaty stipulates otherwise (Sec. 3(2) of the Act 104/2013 Coll.). It means that if the Budapest Convention has any selfexecution provision that stipulates anything else than the law of the CR, this international treaty shall be applied. Unless the Act 104/2013 Coll. stipulates otherwise or in case it does not regulate a certain issue, Code of Criminal Procedure will apply (Sec. 3(1) of the Act 104/2013 Coll.). The Czech Republic applies an European Arrest Warrant vis-a-vis the other EU states.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	***Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended (in particular Section 1 et sequentia and Section 39 et sequentia).*** ***Article 10 of the Constitution of the Czech Republic*** Promulgated international treaties, the ratification of which has been approved by the Parliament and which are binding upon the Czech Republic, shall constitute a part of the legal order; should an international treaty stipulate anything else than a law, the international treaty shall be applied. Procedure according to Act 104/2013 Coll. will apply, unless an international treaty stipulates otherwise (Sec. 3(2) of the Act 104/2013 Coll.). It means that if the Budapest Convention has any selfexecution provision that stipulates anything else than the law of the CR, this international treaty shall be applied. Unless the Act 104/2013 Coll. stipulates otherwise or in case it does not regulate a certain issue, Code of Criminal Procedure will apply (Sec. 3(1) of the Act 104/2013 Coll.).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	The Czech Republic applies a European Investigation Warrant vis-a-vis the other EU states that apliy this legal instrument.
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. 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.	The rules for application of international treaties are described above. ***Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended also stipulete rules for providing of spontagneous information in Sec. 56:*** ***Section 56*** ***Providing Information and Evidence without a Request*** (1) The judicial authority may provide information or evidence from criminal proceedings to a foreign authority without a request for legal assistance, if it believes that it may be utilized in criminal proceedings conducted in the foreign state. Provision of information or evidence must not cause impediments to the purpose of criminal proceedings in the Czech Republic. (2) The judicial authority may set conditions for using the information or evidence in the foreign state. In such a case it will verify at the foreign authority in advance, whether it consents to such conditions. (3) Accordingly to Sub-sections (1) and (2) will the judicial authority proceed in relation to reporting an act that does not fall in the scope of the Criminal Code, but could constitute a criminal offence pursuant to the law of the foreign state.
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.	The Czech Republic applies an European Investigation Warrant vis-a-vis the other EU states that apply this legal instrument. As far as other Council of Europe states that do not aplly the European Investigation Warrant, the Czech Republic applies bilateral treaties or this provision (see Article 10 of the Constitution of the Czech Republic).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the 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	There are also detailed provision on MLA in Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended (in particular Section 1 et sequentia and Section 39 et sequentia). The central authorities are: - the Supreme Public Prosecutor's Office of the Czech Republic for requests from prosecutors - the Ministry of Justice of the Czech Republic for requests from courts

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	The Czech Republic applies the rule of speciality ***Section 7 (2) of the Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended.*** ***Section 7 (2)*** In order to use information or evidence provided to a foreign state for another purpose, than it was provided for, an explicit consent of the judicial or central authority which provided the information or evidence will be necessary, unless an international treaty stipulates otherwise. See above rules for application of international treaties binding upon the Czech Republic and subsidiary use of the Criminal Procedural Code.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	***Section 65 (2) of the Act No. 141/1961 Coll., Code of Criminal Procedure, as amended.*** ***Section 65 (2)*** In pre-trial proceedings, the public prosecutor or the police authority may deny the right to inspect the files, along with the other rights referred to in sub-section (1) based on serious reasons. The public prosecutor is obliged to urgently review the seriousness of the reasons for which the police authority denied these rights upon a request of the person concerned by the refusal. These rights cannot be denied to the accused person and the defense counsel once they have been advised of the possibility to inspect the files, and in the course of negotiating an agreement on the guilt and punishment. ***Section 8a to 8d of the Criminal Procedure Code*** also stipulate the rules for providing information to public about criminal proceedings including restrictions in this area.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or 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.	Expedited preservation of stored computer data – data retention (or preservation) upon the request is regulated in the ***Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended, together with the relevant provisions of the Code of Criminal Procedure – Section 65a and 65b:*** ***Section 65a*** ***Data Retention upon Request of the Czech Republic*** (1) If it is necessary for the purpose of criminal proceedings to secure expedient retention of data stored in a computer system or on a data carrier located in the territory of a foreign state, the unit of the Police of the Czech Republic, which serves as contact point according to an international treaty, (hereafter "Police Unit") will request, with a previous consent of the judicial authority, the foreign authority to retain such data. (2) The data retention request must contain: a) designation of the authority making the request and date of the request, b) brief description of the act subject to criminal proceedings and legal qualification thereof, c) exact designation of the data, retention of which is requested and its relation to the act subject to the criminal proceedings, d) available information necessary to identify the person, in whose possession or under whose control the required data is found, or for identification of the computer system or other data carrier, e) the reason, for which it is necessary to retain the data, and f) information on the fact that the judicial authority intends to file a request for mutual legal assistance or issue an European Investigation Order, in which they will request seizure of the retained data.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(3) Translation of the request referred to in sub-section (2) will be provided by the Police Unit. ***Section 65b*** ***Data Retention upon Request of Foreign State*** (1) If a foreign state authority requests expedient retention of data stored in a computer system or on a data carrier located in the territory of the Czech Republic, the request will be executed, with a previous consent of the judicial authority, by the Police Unit. (2) The competence to grant the consent according to sub-section (1) pertains to the judicial authority, which is competent to proceed according to Part three, Chapter I, Sub-chapter 2 or according to Part five, Chapter XI, Sub-chapter 1 and 2, if the foreign state subsequently sends to the Czech Republic a request for mutual legal assistance or European Investigation Order in seize the retained data. (3) The data retention order will be issued for a limited time period, which must not be shorter than 60 days and longer than 90 days; a new order may be issued upon a justified request of the foreign authority to extend the period by another 90 days. Otherwise Section 7b of the Code of Criminal Procedure will apply accordingly. (4) Requests of a foreign authority for data retention cannot be granted, if the request does not contain the requisites referred to in Section 65a (2) and the foreign authority fails to supplement it even in an additional time period, despite being advised about the consequences associated therewith. (5) If the ascertained circumstances lead to a conclusion that ordering data retention to a certain entity does not sufficiently guarantee future availability of such data or such procedure could lead to leakage of information on criminal proceedings conducted in a foreign state, the Police Unit will immediately notify the foreign state authority and request information, whether they still insists on execution of the request, or whether they withdraw it. (6) The Police Unit will notify the foreign state authority on the manner of execution of their request and advise them that the Czech Republic must receive

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a request for legal assistance or European Investigation Order requesting seizure of the retained data before the time, for which the order was issued, or as the case may be, the extended period according to sub-section (3) expires, otherwise the data will no longer be retained. If the foreign state sends such request or order to the Czech Republic to the judicial authority before the time limit stipulated in the data retention order expires, the data retention period will be extended until the final execution of the request or order by the judicial authority; the judicial authority will immediately notify the person, against whom the order is directed, thereof.
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.	***Section 56 Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended*** ***Section 56*** ***Providing Information and Evidence without a Request*** (1) The judicial authority may provide information or evidence from criminal proceedings to a foreign authority without a request for legal assistance, if it believes that it may be utilized in criminal proceedings conducted in the foreign state. Provision of information or evidence must not cause impediments to the purpose of criminal proceedings in the Czech Republic. (2) The judicial authority may set conditions for using the information or evidence in the foreign state. In such a case it will verify at the foreign authority in advance, whether it consents to such conditions. (3) Accordingly to Sub-sections (1) and (2) will the judicial authority proceed in relation to reporting an act that does not fall in the scope of the Criminal Code, but could constitute a criminal offence pursuant to the law of the foreign state.
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.	The Czech Republic applies an European Investigation Warrant vis-a-vis the other EU states that apply this legal instrument. As far as other Council of Europe states that do not aplly the European Investigation Warrant, the Czech Republic applies bilateral treaties or this provision and provisions of the Act No. 104/2013 Coll., (see Article 10 of the Constitution of the Czech Republic).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	If data are publicly accessible on Internet or a person with full legal capacity provides voluntarily consent to disclose the data, police authority does not need any consent or approval of judicial authority to search Internet.
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.	The Czech Republic applies an European Investigation Warrant vis-a-vis the other EU states that apply this legal instrument. As far as other Council of Europe states that do not aplly the European Investigation Warrant, the Czech Republic applies bilateral treaties or this provision and provisions of the Act No. 104/2013 Coll., (see Article 10 of the Constitution of the Czech Republic). The real-time collection of traffic data can be collected for purposes of the criminal proceedings according to Section 88a of the Criminal Procedural Code.
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	The Czech Republic applies an European Investigation Warrant vis-a-vis the other EU states that apply this legal instrument. As far as other Council of Europe states that do not aplly the European Investigation Warrant, the Czech Republic applies bilateral treaties or this

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	provision and provisions of the Act No. 104/2013 Coll., (see Article 10 of the Constitution of the Czech Republic). The interception of content data for purposes of the criminal proceedings is possible according to Section 88 of the Criminal Procedural Code.
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	24/7 contact point is represented by specialized Cybercrime section, National Agency for Organized Crime, Service of Criminal and Investigation Police. The cybercrime section provides assistance including facilitating, if permitted by its domestic law and practice, directly carrying out the following measures: - the provision of technical advice; - the retention of data – (up to 6 months, according to the Act No. 127/2005 Coll. "Electronic Communications and on Amendment to Certain Related") - the collection of information which can be considered as evidence later (MLAT), the provision of legal information, and locating of suspects. - to issue a request for securing expedient retention (preservation) of data stored in a computer system or on a data carrier located in the territory of a foreign state - with a previous consent of a judicial authority (Sec 65a of the Act No. 104/2013 Coll.), - data Retention (preservation) upon Request of Foreign State - with a previous consent of the judicial authority (Sec 65b of theAct No. 104/2013 Coll.), - carry out communications with the contact points of another Party on an expedited basis. - 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.	

Back to the Table of Contents

Back to the Table of Contents