

MONTENEGRO

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 6 April 2020

[reference to the provisions of the Budapest Convention]

Chapter I - Use of terms

Article 1 - "Computer system", "computer data", "service provider", "traffic data"

Chapter II - Measures to be taken at the national level

Section 1 - Substantive criminal law

Article 2 - Illegal access

Article 3 - Illegal interception

Article 4 - Data interference

Article 5 - System interference

Article 6 - Misuse of devices

Article 7 - Computer-related forgery

Article 8 - Computer-related fraud

Article 9 – Offences related to child pornography

Article 10 – Offences related to infringements of copyright and related rights

Article 11 – Attempt and aiding or abetting

Article 12 - Corporate liability

Article 13 - Sanctions and measures

Section 2 - Procedural law

Article 14 - Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 - Expedited preservation of stored computer data

Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 - Production order

Article 19 – Search and seizure of stored computer data

Article 20 - Real-time collection of traffic data

Article 21 - Interception of content data

Section 3 - Jurisdiction

Article 22 - Jurisdiction

Chapter III – International co-operation

Article 24 - Extradition

Article 25 – General principles relating to mutual assistance

Article 26 – Spontaneous information

Article 27 – Procedures pertaining to mutual assistance requests in the

absence of applicable international agreements

Article 28 - Confidentiality and limitation on use

Article 29 - Expedited preservation of stored computer data

Article 30 - Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer data

Article 32 – Trans-border access to stored computer data with consent or where publicly available

Article 33 - Mutual assistance in the real-time collection of traffic data

Article 34 - Mutual assistance regarding the interception of content data

Article 35 - 24/7 Network

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.



State:	
Signature of the Budapest Convention:	06/04/2005
Ratification/accession:	02/03/2010

DOMESTIC LEGISLATION

Chapter I – Use of terms

Article 1 - "Computer system", "computer data", "service provider", "traffic data":

For the purposes of this Convention:

- "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;
- "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;
- "service provider" means: C
- ability to communicate by means of a computer system, and
- such communication service or users of such service:
- "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.

Art. 142 of the Criminal Code - Meaning of Terms Used in this Code

- (16) A computer system is understood to mean every device or a group of mutually connected or conditioned devices, of which one or several, depending on the programme, perform automatic data processing.
- (17) A computer data is understood to mean any presentation of facts, data or concepts in the form that is suitable for processing in a computer system, including programmes by which a computer system performs its functions.
- (18) A computer programme is understood to mean a set of ordered computer data on the basis of which a computer system performs its functions.
- (19) A computer virus is understood to mean a computer programme which any public or private entity that provides to users of its service the threatens or alters the functions of a computer system and alters, jeopardizes or uses computer data without authorization.
- any other entity that processes or stores computer data on behalf of (20) Computer traffic data are understood to mean all computer data generated by computer systems, which make a chain of communication between two computer systems that communicate, including themselves.
 - (29) The expression "shall not be punished" means that there exists no criminal offence in that case.

Chapter II – Measures to be taken at the national level

Section 1 - Substantive criminal law

Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 - Illegal access

Art. 353 of the Criminal Code – Unauthorized Access to Computer System

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 (2) Where the perpetrator committed the offence under para. 1 above by violating infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected a prison term up to three years. to another computer system.

DOMESTIC LEGISLATION

- (1) Anyone who, without authorization, makes access to the entire computer system or part thereof shall be punished by a fine or a prison term up to one year.
- the measures for computer system protection, he shall be punished by a fine or
- (3) The punishment under para. 2 above shall also apply to anyone who, without authorization, intercepts computer data which are not public, irrespective of the method of their transfer, during their transfer to a computer system, from it or within the system itself, including electromagnetic emission.
- (4) Whoever uses the data obtained in the manner referred to in paras 1, 2 and 3 above shall be punished by a fine or a prison term up to three years.
- (5) Where the offence under para. 4 above resulted in grave consequences for another person, the perpetrator shall be punished by a prison term from six months to five years.

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 (2) Where the offence under para. 1 above results in damage exceeding three committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 349 of the Criminal Code - Damaging Computer Data and **Programs**

- (1) Anyone who without authorization deletes, alters, damages, conceals or otherwise makes useless computer data or program shall be punished by a fine or a prison term up to one year.
- thousand euros, the perpetrator shall be punished by a prison term from three months to three years.
- (3) Where the offence under para. 1 above results in damage exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from three months to five years.
- (4) The devices and means used for the commission of the criminal offences under paras 1, 2 and 3 above shall be confiscated provided that they are owned by the perpetrator.

Article 350 of the Criminal Code - Computer System Interference

BUDAPEST CONVENTION DOMESTIC LEGISLATION (1) Anyone who enters, destroys, deletes, alters, damages, conceals or otherwise makes useless computer data or computer system with the intention to obstruct the operations of a computer system shall be punished by a fine or a prison term up to three years. (2) Where the offence under para. 1 above was committed against data and programs that are significant for state authorities, public services, institutions, business organizations or other entities, the offence shall be punished by a prison term from one to eight years. (3) The devices and means used to commit the criminal offences under paras 1 and 2 above shall be confiscated provided that they are owned by the perpetrator. Article 351 of the Criminal Code - Producing and Entering Computer **Viruses** (1) Anyone who makes a computer virus with the intention of entering it into a computer system of another person shall be punished by a fine or a prison term up to one year. (2) Where the perpetrator entered a computer virus into a computer system of another person and thereby caused damage, he shall be punished by a fine or a prison term up to two years. (3) The device and means used for commission of the criminal offences under paras 1 and 2 above shall be confiscated. **Article 352 of the Criminal Code – Computer Fraud** (1) Anyone who enters, alters, erases, omits to enter correct data or otherwise conceals or misrepresents a piece of computer data or otherwise interferes with the functioning of a computer system and thereby influences the result of electronic processing, transfer of data and functioning of a computer system with the intention of obtaining illicit pecuniary gain for himself or for another person and thereby causes property damage to another person shall be punished by a prison term from six months to five years.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (2) Where the offence under para. 1 above resulted in pecuniary gain exceeding three thousand euros, the perpetrator shall be punished by a prison term from two to ten years. (3) Where the offence under para. 1 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years. (4) Where the offence under para. 1 above was committed with the sole purpose of causing damage to another person, the perpetrator shall be punished by a fine or a prison term up to two years. Article 353 of the Criminal Code - Unauthorized Access to Computer System (1) Anyone who, without authorization, makes access to the entire computer system or part thereof shall be punished by a fine or a prison term up to one year. (2) Where the perpetrator committed the offence under para. 1 above by violating the measures for computer system protection, he shall be punished by a fine or a prison term up to three years. (3) The punishment under para. 2 above shall also apply to anyone who, without authorization, intercepts computer data which are not public, irrespective of the method of their transfer, during their transfer to a computer system, from it or within the system itself, including electromagnetic emission. (4) Whoever uses the data obtained in the manner referred to in paras 1, 2 and 3 above shall be punished by a fine or a prison term up to three years. (5) Where the offence under para. 4 above resulted in grave consequences for another person, the perpetrator shall be punished by a prison term from six months to five years. Article 354 of the Criminal Code – Misuse of Devices and Programs (1) Whoever produces, sells, procures for use, imports, distributes and otherwise places at disposal:

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	 a) devices and computer programs designed or adapted primarily for purposes of commission of the offences under Articles 349 to 353 hereof, b) computer codes or similar data through which one can access the entire computer system or parts thereof with the intention of using it for the purpose of committing the offences under Articles 349 to 353 hereof shall be punished by a prison term from three months to three years.
	(2) Anyone who possesses any of the means under para. 1 above with the intention of using them for the purpose of committing any of the offences under Articles 349 to 353 shall be punished by a fine or a prison term up to one year.
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.	Article 349 of the Criminal Code – Damaging Computer Data and Programs
	(1) Anyone who without authorization deletes, alters, damages, conceals or otherwise makes useless computer data or program shall be punished by a fine
	or a prison term up to one year.
paragraph 1 result in serious harm.	(2) Where the offence under para. 1 above results in damage exceeding three thousand euros, the perpetrator shall be punished by a prison term from three months to three years.
	(3) Where the offence under para. 1 above results in damage exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from three months to five years.
	(4) The devices and means used for the commission of the criminal offences under paras 1, 2 and 3 above shall be confiscated provided that they are owned by the perpetrator.
	Article 351 of the Criminal Code – Producing and Entering Computer Viruses
	(1) Anyone who makes a computer virus with the intention of entering it into a computer system of another person shall be punished by a fine or a prison term up to one year.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (2) Where the perpetrator entered a computer virus into a computer system of another person and thereby caused damage, he shall be punished by a fine or a prison term up to two years. (3) The device and means used for commission of the criminal offences under paras 1 and 2 above shall be confiscated. **Article 352 of the Criminal Code – Computer Fraud** (1) Anyone who enters, alters, erases, omits to enter correct data or otherwise conceals or misrepresents a piece of computer data or otherwise interferes with the functioning of a computer system and thereby influences the result of electronic processing, transfer of data and functioning of a computer system with the intention of obtaining illicit pecuniary gain for himself or for another person and thereby causes property damage to another person shall be punished by a prison term from six months to five years. (2) Where the offence under para. 1 above resulted in pecuniary gain exceeding three thousand euros, the perpetrator shall be punished by a prison term from two to ten years. (3) Where the offence under para. 1 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years. (4) Where the offence under para. 1 above was committed with the sole purpose of causing damage to another person, the perpetrator shall be punished by a fine or a prison term up to two years. **Article 5 - System interference Article 350 of the Criminal Code - Computer System Interference** Each Party shall adopt such legislative and other measures as may be (1) Anyone who enters, destroys, deletes, alters, damages, conceals or otherwise necessary to establish as criminal offences under its domestic law, when makes useless computer data or computer system with the intention to obstruct committed intentionally, the serious hindering without right of the functioning the operations of a computer system shall be punished by a fine or a prison term of a computer system by inputting, transmitting, damaging, deleting, up to three years. deteriorating, altering or suppressing computer data. (2) Where the offence under para. 1 above was committed against data and programs that are significant for state authorities, public services, institutions,

BUDAPEST CONVENTION DOMESTIC LEGISLATION business organizations or other entities, the offence shall be punished by a prison term from one to eight years. (3) The devices and means used to commit the criminal offences under paras 1 and 2 above shall be confiscated provided that they are owned by the perpetrator. Article 351 of the Criminal Code - Producing and Entering Computer Viruses (1) Anyone who makes a computer virus with the intention of entering it into a computer system of another person shall be punished by a fine or a prison term up to one year. (2) Where the perpetrator entered a computer virus into a computer system of another person and thereby caused damage, he shall be punished by a fine or a prison term up to two years. (3) The device and means used for commission of the criminal offences under paras 1 and 2 above shall be confiscated. Article 352 of the Criminal Code - Computer Fraud (1) Anyone who enters, alters, erases, omits to enter correct data or otherwise conceals or misrepresents a piece of computer data or otherwise interferes with the functioning of a computer system and thereby influences the result of electronic processing, transfer of data and functioning of a computer system with the intention of obtaining illicit pecuniary gain for himself or for another person and thereby causes property damage to another person shall be punished by a prison term from six months to five years. (2) Where the offence under para. 1 above resulted in pecuniary gain exceeding three thousand euros, the perpetrator shall be punished by a prison term from two to ten years. (3) Where the offence under para. 1 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) Where the offence under para. 1 above was committed with the sole purpose of causing damage to another person, the perpetrator shall be punished by a fine or a prison term up to two years.
	Article 354 of the Criminal Code – Misuse of Devices and Programs
	(1) Whoever produces, sells, procures for use, imports, distributes and otherwise places at disposal:
	 a) devices and computer programs designed or adapted primarily for purposes of commission of the offences under Articles 349 to 353 hereof, b) computer codes or similar data through which one can access the entire computer system or parts thereof with the intention of using it for the purpose of committing the offences under Articles 349 to 353 hereof shall be punished by a prison term from three months to three years.
	(2) Anyone who possesses any of the means under para. 1 above with the intention of using them for the purpose of committing any of the offences under Articles 349 to 353 shall be punished by a fine or a prison term up to one year.
Article 6 - Misuse of devices	Article 351 of the Criminal Code - Producing and Entering Computer
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:	Viruses (1) Anyone who makes a computer virus with the intention of entering it into a computer system of another person shall be punished by a fine or a prison term
a the production, sale, procurement for use, import, distribution or	up to one year.
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;	(2) Where the perpetrator entered a computer virus into a computer system of another person and thereby caused damage, he shall be punished by a fine or a prison term up to two years.
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,	(3) The device and means used for commission of the criminal offences under paras 1 and 2 above shall be confiscated.
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	

DOMESTIC LEGISLATION

established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 - Computer-related offences

Article 7 – Computer-related forgery

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

Article 352 of the Criminal Code - Computer Fraud

- (1) Anyone who enters, alters, erases, omits to enter correct data or otherwise conceals or misrepresents a piece of computer data or otherwise interferes with the functioning of a computer system and thereby influences the result of electronic processing, transfer of data and functioning of a computer system with the intention of obtaining illicit pecuniary gain for himself or for another person and thereby causes property damage to another person shall be punished by a prison term from six months to five years.
- (2) Where the offence under para. 1 above resulted in pecuniary gain exceeding three thousand euros, the perpetrator shall be punished by a prison term from two to ten years.
- (3) Where the offence under para. 1 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years.
- (4) Where the offence under para. 1 above was committed with the sole purpose of causing damage to another person, the perpetrator shall be punished by a fine or a prison term up to two years.

DOMESTIC LEGISLATION

Article 8 - Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- any input, alteration, deletion or suppression of computer data;
- 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.

Article 352 of the Criminal Code – Computer Fraud

- (1) Anyone who enters, alters, erases, omits to enter correct data or otherwise conceals or misrepresents a piece of computer data or otherwise interferes with the functioning of a computer system and thereby influences the result of electronic processing, transfer of data and functioning of a computer system with the intention of obtaining illicit pecuniary gain for himself or for another person and thereby causes property damage to another person shall be punished by a prison term from six months to five years.
- (2) Where the offence under para. 1 above resulted in pecuniary gain exceeding three thousand euros, the perpetrator shall be punished by a prison term from two to ten years.
- (3) Where the offence under para. 1 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years.
- (4) Where the offence under para. 1 above was committed with the sole purpose of causing damage to another person, the perpetrator shall be punished by a fine or a prison term up to two years.

Title 3 - Content-related offences

Article 9 - Offences related to child pornography

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - through a computer system;
 - computer system;
 - distributing or transmitting child pornography through a computer system;

Article 211 of the Criminal Code - Displaying Pornographic Material to Children and Production and Possession of Child Pornography

- (1) Anyone who sells, shows or publicly exhibits or otherwise makes accessible to a child the texts, pictures, audio-visual material or other objects of pornographic producing child pornography for the purpose of its distribution content or shows the child a pornographic performance shall be punished by a fine or a prison term up to six months.
- offering or making available child pornography through a (2) Anyone who exploits a juvenile to produce pictures, audio-visual material or other objects of pornographic content or for a pornographic performance shall be punished by a prison term from six months to five years.
 - (3) Anyone who procures, sells, shows, attends the display of, publicly exhibits or electronically and otherwise makes available the pictures, audio-visual material

DOMESTIC LEGISLATION

- procuring child pornography through a computer system for oneself or for another person:
- possessing child pornography in a computer system or on a prison term up to two years. computer-data storage medium.
- 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
 - a minor engaged in sexually explicit conduct;
 - a person appearing to be a minor engaged in sexually explicit conduct;
 - realistic images representing a minor engaged in sexually explicit (6) -deletedconduct
- 3 For the purpose of paragraph 2 above, the term "minor" shall include all destroyed. persons under 18 years of age. A Party may, however, require a lower agelimit, 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.

- or other objects of pornographic content resulting from the commission of the acts under para. 2 above, or who possesses such objects shall be punished by a
- (4) If the offences under paras 2 and 3 above were committed against a child, the perpetrator shall be punished for the offence under para. 2 by a prison term from one to eight years, and for the offence under para. 3 by a prison term from six months to five years.
- (5) If the offence under para. 2 above was committed by use of force or threat, the perpetrator shall be punished by a prison term from two to ten years.
- (7) The objects referred to in paras 1 and 3 above shall be confiscated and

Title 4 - Offences related to infringements of copyright and related rights

Article 10 - Offences related to infringements of copyright and related | Article 233 of the Criminal Code - Violation of Moral Rights of Authors rights

- Each Party shall adopt such legislative and other measures as may be (1) Anyone who in his own name or in the name of another person publicizes, in 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 scale and by means of a computer system.
- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the

and Performers

- whole or in part, releases into circulation copies of someone else's copyrighted work or performance or otherwise publicly discloses someone else's copyrighted work or performance shall be punished by a fine or a prison term up to three years.
- (2) Anyone who without a permit of the author changes or re-makes someone such conventions, where such acts are committed wilfully, on a commercial else's copyrighted work or recorded performance shall be punished by a fine or a prison term up to one year.
 - (3) Anyone who releases into circulation copies of someone else's copyrighted work or performance in a manner which is insulting for the author or performer's

infringement of related rights, as defined under the law of that Party, pursuant | honour and reputation shall be punished by a fine or a prison term up to six 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 (4) Objects of the criminal offence and objects that were used for or intended for 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.

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.

DOMESTIC LEGISLATION

months.

- the commission of a criminal offence under paras 1 to 3 above shall be confiscated and objects of the criminal offence shall be destroyed.
- (5) Prosecution for an offence under para. 3 above shall be instituted by a private charge.

Article 234 of the Criminal Code - Unauthorized Use of Copyrighted **Works or Objects of Related Rights**

- (1) Anyone who publicizes, records, duplicates or otherwise publicly discloses or makes available, in whole or in part, a copyrighted work, performance, phonogram, videogram, show or database shall be punished by a prison term up to three years.
- (2) The punishment under para. 1 above shall also imposed on anyone who releases into circulation, or with the intention of releasing into circulation, possesses copies of copyrighted works, performances, phonograms, videograms, shows or databases that have been duplicated or released into circulation without authorization.
- (3) Where the offence under paras 1 and 2 above was committed with the intention of acquiring pecuniary gain for himself or another person, the perpetrator shall be punished by a prison term from three months to five years.
- (4) Instruments for the commission of criminal offences and the instruments that were used for or intended for the commission of the criminal offences under paras 1 and 2 above shall be confiscated, and the objects resulting from the criminal offences shall be destroyed.

Article 235 of the Criminal Code - Voluntary Noncompliance with Protection Measures Intended for Prevention of Violations of Copyright and Related Rights and Rights Related Information

(1) Anyone who produces, imports, releases into circulation, sells, leases, advertises in the interest of sale or leases or keeps for commercial purposes any

BUDAPEST CONVENTION DOMESTIC LEGISLATION devices or means whose basic or main purpose is removal, circumvention or thwarting of technological measures intended for the prevention of violations of copyright and related rights or who uses such devices or means in the interest of violating copyright or related rights shall be punished by fine or a prison term up to three years. (2) Instruments for the commission of criminal offences and the instruments that were used for or intended for the commission of the criminal offence under para. 1 above shall be confiscated, and objects resulting from the criminal offence shall be destroyed. Article 236 of the Criminal Code – Unauthorized Removal or Modification of Electronic Information on Copyright and Related Rights (1) Anyone who without authorization removes or alters electronic information on copyright and related rights, or releases into circulation, imports, broadcasts or otherwise publicly discloses or makes available a copyrighted work or object of related legal protection, from which electronic information on the rights was removed or modified without authorization shall be punished by a fine or a prison term up to three years. (2) Instruments of the criminal offence and the instruments that were used for or intended for the commission of the criminal offences under para. 1 above shall be confiscated, and objects resulting from the criminal offence shall be destroyed. Article 237 of the Criminal Code - Unauthorized Patent Use (1) Anyone who without authorization produces, imports, exports, offers in view of releasing into circulation, releases into circulation, stores or uses in commercial transactions a product or procedure protected by patent shall be punished by a fine or a prison term up to three years. (2) Where the offences under para. 1 above resulted in pecuniary gain or damage exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from one to eight years. (3) Whoever without authorization publicizes or otherwise makes available the

essence of someone else's reported invention before the invention was made

BUDAPEST CONVENTION DOMESTIC LEGISLATION public in the manner laid down by law shall be punished by a fine or a prison term up to two years. (4) Whoever without authorization files a patent application or does not indicate the inventor in the application or indicates him falsely shall be punished by a prison term from six months to five years. (5) Instruments for the commission of criminal offences and instruments that were used for or intended for the commission of the criminal offences referred to in paras 1 to 3 above shall be confiscated, and objects resulting from the criminal offence shall be destroyed. Article 238 of the Criminal Code - Misuse of Design (1) Anyone who without authorization uses, in whole or in part, someone else's registered or protected product design on their traded product shall be punished by a fine or a prison term up to three years. (2) Anyone who without authorization publicizes or otherwise makes available to the public the subject of someone else's design application before it was published in the manner laid down by law shall be punished by a fine or a prison term up to one year. (3) Instruments for the commission of criminal offences and the instruments that were used for or intended for the commission of the criminal offences under para.

Title 5 - Ancillary liability and sanctions

shall be destroyed.

Article 11 - Attempt and aiding or abetting

- 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

Article 20 of the Criminal Code – Attempt

1 Each Party shall adopt such legislative and other measures as may be (1) Anyone who commences the commission of a criminal offence with wrongful intent but does not complete it shall be punished for attempted criminal offence punishable under law by a prison term of five years or longer, whereas other attempted criminal offences shall only be punishable where it is explicitly provided for by law that the punishment also applies to an attempt.

1 above shall be confiscated, and the objects resulting from the criminal offence

DOMESTIC LEGISLATION

committed intentionally, an attempt to commit any of the offences established (2) Also considered to be the commencement of a crime is the use of a specific 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.

- tool or the application of a specific method of commission provided that they are defined by law as elements of the crime.
- (3) A perpetrator shall be punished for an attempt by the punishment laid down for the criminal offence but may also receive a lighter punishment.

Article 21 of the Criminal Code - Inappropriate Attempt

Where a perpetrator attempted to commit a criminal offence with an inappropriate tool or against an inappropriate object punishment may be remitted.

Article 23 of the Criminal Code – Principal and Co-principal

- (1) A principal shall be a person who commits a criminal offence himself or a person who carries out the crime through another person provided that this other person cannot be considered to be the principal.
- (2) Where several persons jointly take part in the commission of a crime with wrongful intent or by negligence, or where they follow their prior arrangement and jointly act with wrongful intent and thus make a significant contribution to the commission of the criminal offence, each person shall receive a punishment prescribed for the crime in question.

Article 24 of the Criminal Code – Instigation

- (1) Anyone who acts with wrongful intent to instigate another person to commit a criminal offence shall receive a punishment as if he committed the crime by himself.
- (2) Anyone who acts with wrongful intent to instigate another person to commit a criminal offence which carries a five-year prison term or a more severe punishment but does not even attempt commission shall receive the punishment laid down by law for the attempted criminal offence.

BUDAPEST CONVENTION DOMESTIC LEGISLATION Article 25 of the Criminal Code - Aiding (1) Anyone who acts with wrongful intent to aid another in the commission of a criminal offence shall be punished as if he committed it himself but may receive a lighter punishment. (2) The following, in particular, shall be considered as aiding in the commission of a criminal offence: giving counsel or instructions on how to commit the crime, supplying the perpetrator with the means for commission of the crime, creating conditions or removing obstacles to the commission of crime as well as promising one prior to the commission to conceal the crime, a perpetrator, the means by which the crime was committed, any traces of the crime, or the proceeds of crime. Article 26 of the Criminal Code - Limits of Liability and Punishment of **Accomplices** (1) Co-principal liability is defined by his wrongful intent or negligence, and instigator and aider liability by their wrongful intent. (2) Where a co-principal, instigator or an aider voluntarily prevented the commission of a criminal offence, punishment may be remitted. (3) Personal relations, capacity and circumstances for which the law excludes culpability or allows for the remission of punishment and which serve as ground to qualify an offence as serious or minor, or have an impact on the punishment imposed, may apply only to the principal, co-principal, instigator or aider with whom such relations, capacity and circumstances exist. Article 12 - Corporate liability Law on Liability of Legal Persons for Criminal Acts (Official Gazette of the Republic of Montenegro no. 2/07, 13/07 and 39/2016). 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 power of representation of the legal person; а an authority to take decisions on behalf of the legal person; b

DOMESTIC LEGISLATION

- c an authority to exercise control within the legal person.
- 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
- 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
- 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 - Sanctions and measures

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
- 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Article 349 of the Criminal Code – Damaging Computer Data and Programs

- (1) Anyone who without authorization deletes, alters, damages, conceals or otherwise makes useless computer data or program shall be punished by a fine or a prison term up to one year.
- (2) Where the offence under para. 1 above results in damage exceeding three thousand euros, the perpetrator shall be punished by a prison term from three months to three years.
- (3) Where the offence under para. 1 above results in damage exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from three months to five years.
- (4) The devices and means used for the commission of the criminal offences under paras 1, 2 and 3 above shall be confiscated provided that they are owned by the perpetrator.

Article 350 of the Criminal Code – Computer System Interference

(1) Anyone who enters, destroys, deletes, alters, damages, conceals or otherwise makes useless computer data or computer system with the intention to obstruct the operations of a computer system shall be punished by a fine or a prison term up to three years.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (2) Where the offence under para. 1 above was committed against data and programs that are significant for state authorities, public services, institutions, business organizations or other entities, the offence shall be punished by a prison term from one to eight years. (3) The devices and means used to commit the criminal offences under paras 1 and 2 above shall be confiscated provided that they are owned by the perpetrator. Article 351 of the Criminal Code - Producing and Entering Computer Viruses (1) Anyone who makes a computer virus with the intention of entering it into a computer system of another person shall be punished by a fine or a prison term up to one year. (2) Where the perpetrator entered a computer virus into a computer system of another person and thereby caused damage, he shall be punished by a fine or a prison term up to two years. (3) The device and means used for commission of the criminal offences under paras 1 and 2 above shall be confiscated. Article 352 of the Criminal Code - Computer Fraud (1) Anyone who enters, alters, erases, omits to enter correct data or otherwise conceals or misrepresents a piece of computer data or otherwise interferes with the functioning of a computer system and thereby influences the result of electronic processing, transfer of data and functioning of a computer system with the intention of obtaining illicit pecuniary gain for himself or for another person and thereby causes property damage to another person shall be punished by a prison term from six months to five years. (2) Where the offence under para. 1 above resulted in pecuniary gain exceeding three thousand euros, the perpetrator shall be punished by a prison term from two to ten years.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Where the offence under para. 1 above resulted in pecuniary gain exceeding thirty thousand euros, the perpetrator shall be punished by a prison term from two to twelve years.
	(4) Where the offence under para. 1 above was committed with the sole purpose of causing damage to another person, the perpetrator shall be punished by a fine or a prison term up to two years.
	Article 353 of the Criminal Code – Unauthorized Access to Computer System
	(1) Anyone who, without authorization, makes access to the entire computer system or part thereof shall be punished by a fine or a prison term up to one year.
	(2) Where the perpetrator committed the offence under para. 1 above by violating the measures for computer system protection, he shall be punished by a fine or a prison term up to three years.
	(3) The punishment under para. 2 above shall also apply to anyone who, without authorization, intercepts computer data which are not public, irrespective of the method of their transfer, during their transfer to a computer system, from it or within the system itself, including electromagnetic emission.
	(4) Whoever uses the data obtained in the manner referred to in paras 1, 2 and 3 above shall be punished by a fine or a prison term up to three years.
	(5) Where the offence under para. 4 above resulted in grave consequences for another person, the perpetrator shall be punished by a prison term from six months to five years.
	Article 354 of the Criminal Code – Misuse of Devices and Programs
	(1) Whoever produces, sells, procures for use, imports, distributes and otherwise places at disposal:
	 a) devices and computer programs designed or adapted primarily for purposes of commission of the offences under Articles 349 to 353 hereof, b) computer codes or similar data through which one can access the entire computer system or parts thereof with the intention of using it for the

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	purpose of committing the offences under Articles 349 to 353 hereof shall be punished by a prison term from three months to three years.
	(2) Anyone who possesses any of the means under para. 1 above with the intention of using them for the purpose of committing any of the offences under Articles 349 to 353 shall be punished by a fine or a prison term up to one year.
Section 2 – Procedural law	

Article 14 - Scope of procedural provisions

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
- 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
 - the criminal offences established in accordance with Articles 2 through 11 of this Convention;
 - other criminal offences committed by means of a computer system; and
 - 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 Article 20.
- 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:
 - is being operated for the benefit of a closed group of users, and

Article 75 of the CPC - Reasons for Search of Dwellings, Other Premises, **Movable Articles and Persons**

- (1) Search of dwellings and other premises of the accused persons or other persons as well as their movable articles outside the dwellings may be carried out if grounds for suspicion exist that in the course of search the perpetrator would be caught or that traces of the criminal offence or objects relevant to the criminal procedure would be found.
- (2) The search of movable articles within the meaning of paragraph 1 of this Article shall include the search of computers and similar devices for automatic data processing to which the computer is connected. At the request of the court, the person using a computer shall enable access to the computer and removable storage used for storing information relative to the object of the search (discs, USB flash discs, USB hard discs, diskettes, tapes and alike), as well as give necessary information on the use of the computer. Persons who refuse to do so although reasons referred to in Article 111 of the present Code do not exist may be punished pursuant to Article 85 paragraph 3 of the present Code.
- a reservation to enable the broadest application of the measure referred to in (3) Search of persons may be carried out if grounds for suspicion exist that in the course of search traces and objects relevant to the criminal procedure would be found.

Article 76 of the CPC - Search Warrant and Request for a Search Warrant

(1) A search warrant shall be issued by the court at the request of the State Prosecutor or at the request of an authorized police officer granted authorization by the State Prosecutor, and it shall be enforced by the police.

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.

DOMESTIC LEGISLATION

(2) A request for the issuance of a search warrant shall be submitted in writing, and only exceptionally orally in line with Article 78 of the present Code.

Article 77 of the CPC – Contents of the Request for a Search Warrant

The request for issuing a search warrant shall contain:

- 1) the name of the applicant,
- 2) the name of the court to which the request is addressed,
- 3) facts indicating the likelihood that reasons for search exist referred to in Article 75 of the present Code,
- 4) the first and the last name, and, if necessary, a description of the person to be apprehended during the search of dwellings or other premises, or expected traces and a description of objects that should be found by the search,
- 5) the designation of the location of the search, by indicating the address, information about the owner or the person in possession of the objects, dwellings or other premises and any other information of importance to establish the identity, and
- 6) signature of the applicant.

Article 78 of the CPC – Verbal Request for a Search Warrant

- (1) A verbal request for issuing a search warrant may be filed when risk of delay exists.
- (2) The request from paragraph 1 of this Article may be communicated to the investigating judge also by telephone, radio or other means of electronic communication.
- (3) When a verbal request for issuing a search warrant has been submitted, the investigating judge shall record the further course of conversation. If a voice recording device has been used or stenographic records kept, a transcription thereof shall be made within 24 hours, the identity of which shall be certified and kept with the original records.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 79 of the CPC – Search Warrant
	(1) When the investigating judge receives the request for issuing a search warrant, if s/he agrees with the request, s/he shall immediately issue a search warrant containing:
	1) the information provided for in Article 77 of the present Code;
	2) that the search will be conducted by the police;
	3) an instruction that the search is being done in accordance with Article 80 of the present Code;
	4) signature of the judge and the official stamp of the court.
	(2) If the investigating judge determines that the request for issuing a search warrant is not justified, s/he shall immediately request the panel referred to in Article 24, paragraph 7 of the present Code to decide on the request. The panel shall make a decision within 24 hours.
	Article 80 of the CPC – Search Upon a Court Order
	(1) Before the commencement of the search, the search warrant shall be given to the person to be searched or whose premises are to be searched. Before the search, the persons against whom the search warrant has been issued shall be asked to voluntarily hand over the wanted person or objects. Those persons shall be instructed that they are entitled to retain a lawyer i.e. a defence attorney who may be present during the search. If a person against whom a search warrant has been issued demands the presence of a lawyer or defence attorney, the commencement of the search shall be postponed until his/her arrival, but for no more than two hours.
	(2) The search may commence without previously presenting a warrant or without a previous invitation to hand over the person or objects and without an instruction on the right to a defence attorney or lawyer, if it is necessary in order to prevent a criminal offence from being committed, for the purpose of outright capture of a criminal offender, saving of persons and property or if the search is to be carried out in public premises.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (3) The search shall be carried out by day from 6:00h until 21:00h. The search may be carried out by night as well, if it was commenced during the day and was not completed or if it was explicitly ordered so by the court because of risk of delay or if reasons referred to in Article 83 paragraph 1 of the present Code exist. Article 81 of the CPC - Rules of Search (1) The occupants of a dwelling or other premise shall be summoned to attend the search, and if they are absent, their representative, adult members of his family or neighbours shall be summoned to attend. (2) Premises that are locked, furniture and other things shall be opened by force only if their occupant is absent or if the occupant is refusing to open them voluntarily. Unnecessary damage shall be avoided in the course of opening. (3) The search of a dwelling or person shall be attended by two citizens of age in the capacity of witnesses, unless reasons referred to in Article 83 paragraph 4 of the present Code exist. The search of persons shall be carried out by a person of the same sex, and a person of the same sex shall be taken as a witness. Before the commencement of the search, witnesses shall be admonished to pay attention to the course of the search, as well as that they have the right to raise their objections before the signing of the record on the search, should they consider that the contents of the record are incorrect. (4) When conducting a search of premises of state authorities, enterprises or other legal entities, a head of such authorities, enterprises or other legal entities shall be summoned to be present at the search. (5) Search and inspections of military facilities shall be carried out upon the permission of the competent military officer and in the presence of a person designated by him/her. (6) If a search needs to be carried out aboard a ship or aircraft the search warrant shall be delivered to the captain of the ship or person in charge of the aircraft. The captain of the ship or the person in charge of aircraft, or a person designated by them shall witness the search.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (7) The search of dwellings and persons shall be carried out carefully, while respecting human dignity and the right to privacy, without unnecessary disturbance of the house rules and without causing nuisance to the citizens. (8) A record shall be made on the search signed by the person whose premises have been searched or who has been searched and by persons whose attendance at the search is mandatory. The course of the search may be audio and audiovisually recorded while paying special attention to the places where certain persons and objects have been found. The venue of the search and its individual parts, as well as the persons or objects found during the search may be photographed. Audio or audio-visual recordings and photographs shall be enclosed to the record on the search and may be used as evidence. (9) Only those objects and documents that relate to the purpose of the search shall be provisionally seized in the course of the search. The records shall include and clearly specify the objects and documents that have been seized, which shall also be indicated in a receipt to be given immediately to the person from whom the objects or documents have been seized. Article 82 of the CPC - Seizure of Other Objects on Basis of a Search Warrant (1) If a search of a dwelling or a person reveals objects that are unrelated to the criminal offence for which the search was ordered, but indicate the commission of another criminal offence that is prosecuted by virtue of office, they shall be described in the record and provisionally seized, and a receipt confirming seizure shall be issued immediately. (2) If the search was not attended by the competent State Prosecutor, s/he shall immediately be informed about the discovery of objects referred to in paragraph 1 of this Article for the purpose of initiating criminal procedure. These objects shall be returned immediately if the State Prosecutor establishes that there are no grounds to initiate criminal proceedings and if no other legal grounds for the seizure of these objects exist. (3) If certain objects are seized during the search of computers and similar

devices for automatic data processing, they shall be immediately returned to their

BUDAPEST CONVENTION DOMESTIC LEGISLATION users, if they are not needed for further procedure. Personal information obtained during the search may be used only for the purposes of conducting a criminal procedure and shall be erased as soon as that purpose ceases. Article 83 of the CPC - Entering Another Person's Dwellings without a **Search Warrant and Searching** (1) An authorized police officer may enter another person's dwelling or other premises without a court order and, if necessary, carry out the search, if the tenant so requires or if somebody is seeking help or if it is necessary for the purpose of preventing the commission of a criminal offence or direct capturing of a criminal offender, or for the purpose of saving people and property, enforcement of a decision on detention or bringing in the accused person or other person, or for the purpose of deprivation of liberty of a criminal offence perpetrator who is on the run or a person from the arrest warrant, or if the search is to be carried out in public premises. (2) The tenant, if present, shall have the right to object to the procedure of the authorized police officer referred to in paragraph 1 of this Article. The authorized police officer shall inform the tenant about this right and shall include his/her objections in the receipt on entering the dwelling or in the search record. (3) In case referred to in paragraph 1 of this Article, if another person's dwelling was only entered without search, the tenant shall be issued a receipt stating the reason for entering the dwelling or other premises as well as the tenant's objections. If search was also carried out in another person's dwelling or other premises, the procedure shall be the one referred to in Article 81, paras. 3, 7 and 8 and Article 82, paragraph 1 of the present Code. (4) A search may also be carried out without the presence of witnesses if their presence during the search would expose the witnesses to risk of physical injuries or if it is not possible to arrange their presence immediately, and risk of delay exists. The reasons for the search without the presence of witnesses shall be specified in a record. (5) Authorized police employees may, without a search warrant and without the

presence of witnesses, carry out a search of persons when enforcing a warrant on

BUDAPEST CONVENTION DOMESTIC LEGISLATION compulsory apprehension or when depriving of liberty, if suspicion exists that the person owns weapons or dangerous tools, or if suspicion exists that the person would reject, hide or destroy the objects that need to be taken from him/her as evidence in a criminal procedure. (6) If there are grounds for suspicion that criminal offence was committed that is prosecuted by virtue of office, authorized police employees may, without a court warrant and without the presence of witnesses, carry out the search of transport means, passengers, luggage and other movable objects, with the exception of things referred to in Article 75 paragraph 2 of the present Code. (7) When conducting a search without a search warrant, authorized police officers shall immediately submit thereon a report to the investigative judge. **Article 84 of the CPC – Legally Invalid Evidence** If the search was conducted in contravention to the provisions of Article 76, Article 80 paragraph 1, Article 81 paragraph 3 and Article 83 of the present Code, search records and evidence collected during the search may not be used as evidence in the course of criminal procedure. Article 85 of the CPC - Provisional Seizure of Objects and Property Gain (1) Objects which have to be seized according to the Criminal Code or which may be used as evidence in the criminal procedure, shall, at the proposal of a State Prosecutor, and by way of a court ruling, be provisionally seized and delivered for safekeeping to the court or their safekeeping shall be secured in another way. (2) The ruling on the provisional seizure of objects shall contain: 1) the name of the court rendering the ruling; 2) legal grounds for the seizure of objects; 3) indication and description of objects that are to be provisionally seized, and 4) the first and the last name of the person from whom the object is provisionally seized and the place at or in which a certain object should be provisionally seized.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (3) Anyone who is in possession of objects referred to in paragraph 1 of this Article shall hand them over. Persons refusing to hand over the objects may be punished by a fine of up to €1.000, and in case of further rejection, they may be detained. Detention shall last until the object is handed over or until the criminal procedure is completed, and at the longest for two months. The procedure as regards a person in an official capacity or a responsible person in a public authority, enterprise or another legal entity shall be the same. (4) Provisions of paras. 1 and 3 of this Article shall be applied to the data saved in devices for automatic or electronic data processing and media wherein such data are saved, which shall, upon the request of the court, be handed over in a legible and comprehensible form. The court and other authorities shall abide by the regulations on maintaining data secrecy. (5) The following objects cannot be provisionally seized: 1) papers and other documents of public authorities, publication of which would violate the obligation to keep data secret in terms of regulations laying down data secrecy, until the competent authority decides otherwise; 2) the accused persons' letters to their defence attorney or the persons referred to in Article 109, paragraph 1, items 1, 2 and 3 of the present Code unless the accused decide to hand them over voluntarily; 3) recordings, extracts from the register and similar documents that are in possession of persons referred to in Article 108, item 3 of the present Code and that are made by such persons in relation to the facts obtained from the accused person while performing their professional service, if publication thereof would constitute violation of the obligation to keep a professional secret. (6) The prohibition referred to in paragraph 5, item 2 of this Article shall not apply to the defence attorney or persons exempted from the duty to testify pursuant to Article 109, paragraph 1 of the present Code if reasonable doubt exists that they aided the accused parties in committing the criminal offence or they helped them after the criminal offence was committed or if they acted as accomplices by virtue of concealment.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(7) The ruling referred to in paragraph 3 of this Article shall be made by the investigative judge during the investigation and by the Chair of the Panel after an indictment has been brought.
	(8) The panel referred to in Article 24, paragraph 7 of the present Code shall decide on the appeal against a ruling referred to in paras. 2 and 3 of this Article. An appeal against the ruling on imprisonment shall not stay the execution.
	(9) Authorized police employees may seize objects referred to in paragraph 1 of this Article when proceeding pursuant to Articles 257 and 263 of the present Code or when executing a court warrant.
	(10) When seizing objects, it shall be indicated where they were found and they shall be described, and where appropriate, their identity shall be established in another way as well. A receipt shall be issued for the seized objects.
	(11) Measures referred to in paragraph 3 of this Article may not be enforced against the suspects or accused parties or persons relieved of duty to testify.
	(12) Provision of Article 481 of the present Code shall be applied on the provisional seizure of property gain.
	Article 86 of the CPC - Denial of Disclosure or Issuing of Files
	(1) State authorities may refuse to disclose or issue their files and other documents if they deem that disclosure of their contents would cause damage to the public interests, with the exception of case of seizing the property gained through criminal activity. If disclosure or handover of files and other documents was denied, the final decision shall be made by the panel referred to in Article 24, paragraph 7 of the present Code.
	(2) Enterprises or other legal entities may request that data related to their business operations are not publicly disclosed. The panel referred to in Article 24 paragraph 7 of the present Code shall decide on the request.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 87 of the CPC – Inventory and Sealing of Files
	(1) An inventory of provisionally seized files that may be used as evidence shall be made. If that is not possible, the files shall be put in a cover and sealed. The owner of the files may put his/her seal on the cover.
	(2) The person from whom the files have been seized shall be summoned to attend the opening of the cover. If this person fails to appear or is absent, the cover shall be opened, the files examined and a list of them made in his/her absence.
	(3) During the examination of files, attention shall be paid that their contents are not be disclosed to unauthorized persons.
	Article 89 of the CPC - Obtaining Information from the Competent Public Authority for Temporary Suspension of Monetary Transactions
	(1) State Prosecutors may request that the competent public authority performs control over the financial operations of certain persons and to submit them documentation and information which can be used as evidence of a criminal offence or of the proceeds of crime, as well as information about suspicious monetary transactions.
	(2) State Prosecutors may request that the competent authority or organization temporarily suspends the payment, or the issuing of suspicious money, securities and objects, at the longest for six months.
	(3) State Prosecutors shall specify in the motion referred to in paragraphs 1 and 2 of this Article in more detail the contents of measure of action they are requesting.
	(4) At the proposal of State Prosecutors, the court may issue a ruling ordering a temporary suspension of a certain monetary transaction when reasonable doubt exists that it constitutes a criminal offence or that it is intended for the commission or concealment of a criminal offence or proceeds of crime.
	(5) By way of the ruling referred to in paragraph 4 of this Article, the court shall order that funds in check or cash form be provisionally seized and deposited into

BUDAPEST CONVENTION DOMESTIC LEGISLATION a special account where they will be kept until the completion of the proceedings with final force and effect or until conditions for their return are met. (6) An appeal against the ruling referred to in paragraph 4 of this Article may be filed by the parties and the defense attorney, or the owner of funds or his/her proxy or the legal person from whom the funds have been provisionally seized. Such an appeal shall be decided upon by the panel referred to in Article 24, paragraph 6 of the present Code. Article 157 of the CPC - Types of Secret Surveillance Measures and **Conditions for their Application** (1) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of the present Code and evidence cannot be obtained in another manner or their obtaining would require a disproportional risk or endangering the lives of people, measures of secret surveillance may be ordered against those persons: Secret surveillance and recording of telephone conversations and other distance communication; • Interception, collection and recording of computer data: Entry into premises for the purpose of secret photographing and video and audio recording in premises; Secret following and video and audio recording of persons and objects. (2) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of the present Code and circumstances of the case indicate that evidence shall be collected with a minimum violation of the right to privacy, measures of secret surveillance may be ordered against those persons: 1. Simulated purchase of objects or persons and simulated giving and taking of bribe; 2. Providing simulated business services or concluding simulated legal transactions;

3. Establishing fictitious companies;

BUDAPEST CONVENTION DOMESTIC LEGISLATION 4. Supervision over the transportation and delivery of objects of criminal offence; 5. Recording conversations upon previous informing and obtaining the consent of one of interlocutors: 6. Hiring undercover investigators and collaborators. (3) Measures referred to in paragraph 1, item 1 of this Article may be also ordered against persons for whom there are grounds for suspicion that they have been conveying to the perpetrator or from the perpetrator of criminal offences referred to in Article 158 of the present Code messages in connection to the criminal offence, or that the perpetrator has been using their telephone lines or other electronic communication devices. (4) In the case where there is no knowledge about the identity of the perpetrator of the criminal offence, the measures referred to in paragraph 1, item 4 of this Article may be ordered against the object of the criminal offence. (5) No criminal prosecution shall be undertaken against the persons who carry out the measures referred to in paragraph 2, items 1, 2, 5 and 6 of this Article, for acts which constitute aiding in committing a criminal offence, if it is done in order to provide information and evidence for the successful conduct of criminal proceedings. (6) Enforcement of measures referred to in paragraph 2, items 1, 2, 5 and 6 of this Article shall not constitute incitement to commit a criminal offence. (7) The measures referred to in paragraph 1, items 1 to 4 of this Article and measures referred to in paragraph 2, items 5 and 6 of this Article may be ordered against a person for whom an international arrest warrant was issued, or against a third party for whom there are grounds for suspicion that he is in direct contact with the person for whom there is an international arrest warrant. Article 158 of the CPC - Criminal Offences for Which Measures of Secret **Surveillance May Be Ordered** The measures referred to in Article 157 of the present Code may be ordered for the following criminal offences:

BUDAPEST CONVENTION DOMESTIC LEGISLATION 1) for which a prison sentence of ten years or a more severe penalty may be imposed; 2) having elements of organized crime; 3) causing false bankruptcy, abuse of assessment, passive bribery, active bribery, trading in influence, abuse of an official position, as well as abuse of powers in economy, and fraud in the conduct of an official duty with prescribed imprisonment sentence of eight years or a more severe sentence; 4) abduction, extortion, blackmail, meditation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of evidences, criminal association, disclosure of confidential information, breach of confidentiality of proceedings, money laundering, counterfeiting of money, forgery of documents, falsification of official documents, making, procuring or providing to others means and materials for forging, participation in foreign armed formations, arranging outcomes of competitions., unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beinas. 5) against the security of computer data. Article 159 of the CPC - Competence for Ordering Measures of Secret Surveillance and their Duration (1) Measures referred to in Article 157, paragraph 1 of the present Code shall be ordered via a written order by the investigative judge at the motion of the State Prosecutor containing a statement of reasons. The measures referred to in Article 157, paragraph 2 of the present Code shall be ordered by the State Prosecutor, at the reasoned motion of an authorized police officer or ex-officio, via a written order. The motion containing a statement of reasons shall be delivered in a closed envelope bearing the designation MSS - Measures of Secret Surveillance. (2) The motion and the order referred to in paragraph 1 of this Article shall contain: the type of measure, data on the person against whom the measure is

enforced if this person is known, grounds for reasonable suspicion, the manner of

BUDAPEST CONVENTION DOMESTIC LEGISLATION measure enforcement, its goal, scope and duration. If it is a measure of engagement of an undercover agent and collaborator, the motion and the order shall also contain the use of false documents and technical devices for the transfer and recording of voice, image and video, participation in the conclusion of legal affairs, as well as the reasons justifying the engagement of a person who is not a police officer as an undercover agent and cooperative witness. (3) The motion and the order for ordering measures shall become an integral part of the criminal file and should contain available data on the person against whom they are ordered, the criminal offence because of which they are ordered, facts on basis of which the need to undertake them originates, duration deadline that needs to be suitable to achieving the objective of measure, manner, scope and place for the measures to be implemented (4) By way of exception, if the written order cannot be issued in time and risk of delay exists, application of measure referred to in Article 157 of the present Code may begin on basis of a verbal order of the investigative judge, i.e., State Prosecutor. In that case, a written order must be obtained within 12 hours following the issue of the verbal order. (5) Based on the order of the investigating judge or State Prosecutor, the measures referred to in Article 157, paragraph 1 and paragraph 2, items 3 to 6 of the present Code may last up to four months. For justified reasons, these measures may be extended against the same person and for the same criminal offence no longer than 18 months from the adoption of the first order for imposing secret surveillance measures. Enforcement of the measures shall be terminated by an order when the reasons for their application cease. Measures whose enforcement was interrupted may continue for justified reasons against the same person and for the same criminal offence, based on an order. The maximum duration of the measure also includes the time during which the measure was interrupted. After the expiry of the periods referred to in this paragraph, enforcement of a measure may not continue, and new measures may not be ordered for the same criminal offence and against the same perpetrator. The motion for undertaking the measure referred to in Article 157, paragraph 2, items 1 and 2 of the present Code may refer only to one simulated act, and all

subsequent motions for the application of this measure against the same person

BUDAPEST CONVENTION DOMESTIC LEGISLATION shall contain a statement of reasons justifying the repeated application of this measure. (6) If during the enforcement of the measure it shows out that the measure cannot achieve the intended purpose, it may be replaced by another measure. The maximum duration of the newly ordered measure shall include the duration of the previously ordered measures. (7) Ordering secret surveillance measures referred to in Article 157 para. 1 and 2 of the present Code against the same person and for the same criminal offence shall not affect the ordering of secret surveillance measures against a person for whom an international arrest warrant was issued or against a third party for whom there is reasonable suspicion that they are in direct contact with the person for whom there is an international arrest warrant. (8) In addition to the order for the application of measure referred to in Article 157, paragraph 1, item 1 of the present Code, the investigative judge shall issue a separate order containing solely the telephone number or e-mail address or the International Mobile Subscriber Identity (IMSI number), International Mobile Station Equipment Identity (IMEI number) and the internet protocol address (IP address) and the duration of the measure in question, and this order shall be delivered to enterprises referred to in paragraph 6 of this Article during the course of the application of the measure by the authorized police officers. (9) Postal agencies, other enterprises and legal entities registered for transmission of information shall enable the authorized police officers to enforce the measure referred to in Article 157, paragraph 1 of the present Code. Persons acting in an official capacity and responsible persons involved in the process of passing the order and enforcement of the measures referred to in Article 157 of the present Code shall keep as secret all the data they have learned in the course of this procedure. (10) If, during the enforcement of measures of secret surveillance, data and notifications are registered referring to some other persons for whom grounds for suspicion exist that s/he had committed the criminal offence for which a measure of secret surveillance was ordered, or some other criminal offence, that part of

the material shall be copied and forwarded to the State Prosecutor, and it may

BUDAPEST CONVENTION DOMESTIC LEGISLATION be used as evidence only for criminal offences referred to in Article 158 of the present Code. (11) The State Prosecutor and the investigative judge shall, in an appropriate way (by coping records or official annotations without personal data, removal of an official annotation from the files and alike), prevent unauthorised persons, the suspects or their defence attorney to establish the identity of persons who have enforced the measures referred to in Article 157 of the present Code, as well as undercover agent and cooperative witness. If such persons are to be heard as witnesses, the court shall act in the manner prescribed in Articles 120-123 of the present Code. Article 160 of the CPC - Enforcement of Measures of Secret Surveillance (1) The measures referred to in Article 157 of the present Code shall be enforced by the authorized police officers in such a manner that the privacy of persons not subject to these measures be disturbed to the least extent possible. (2) Undercover agent and collaborator may be an authorized police officer, employee in another public authority, authorized police officer of another state or, by way of exception, if the measure cannot be enforced in another manner, some other person. An undercover investigator shall be designated by the head of the body responsible for enforcement of secret surveillance measures or a person authorized by him. (3) Undercover agents and cooperative witnesses cannot be persons for whom reasonable suspicion exists that they were or that they currently are members of a criminal organization or group or persons who have been sentenced for criminal offences organized crime. (4) Undercover investigator and collaborator may participate in legal transactions by using false documents to conceal their identity, and when collecting information, they may use technical devices for the transfer and recording of sound, image and video. The body responsible for issuance of documents on the basis of which a person's identity may be established shall, at the request of the head of the body responsible for enforcement of secret surveillance measures,

BUDAPEST CONVENTION DOMESTIC LEGISLATION issue documents for concealing the identity of a police officer and other persons, entering into the database data from these documents. (5) Authorised police officer enforcing the measure shall keep records on each measure undertaken and report periodically to the State Prosecutor, that is, investigative judge on the enforcement of measures. If the State Prosecutor, i.e., investigative judge ascertains that the need for enforcement of the ordered measures does not exist anymore, s/he shall issue and order on their discontinuation. (6) Upon the enforcement of measures referred to in Article 157 of the present Code the authorized police officers shall submit to the State Prosecutor a final report and other material obtained by the enforcement of measures. (7) Should the State Prosecutor decide not to initiate a criminal procedure or if the data and information collected via secret surveillance measures are not necessary for the criminal proceedings, s/he shall forward to the investigative judge the material obtained through the application of Article 157 of the present Code, in a closed cover bearing the designation MSS, and the investigative judge shall order that the material be destroyed in the presence of the State Prosecutor and the investigative judge. The investigative judge shall compose a record thereon. (8) The investigative judge shall proceed in the manner described in paragraph 7 of this Article if the State Prosecutor orders that investigation be conducted against the suspect who was subjected to measures of secret surveillance, when the results obtained or parts of the results are not indispensable for the conduct of the criminal proceedings or when the person for whom there is an international arrest warrant is found. (9) In cases referred to in paras. 7 and 8 of this Article, data shall be considered as classified within the meaning of regulation prescribing data secrecy. (10) The manner of production, use, keeping and destroying documents for establishing identity shall be governed by an act of the ministry responsible for internal affairs.

BUDAPEST CONVENTION DOMESTIC LEGISLATION Article 161 of the CPC - Legally Invalid Evidence (1) If the measures referred to in Article 157 of the present Code were undertaken in contravention to the provisions of the present Code or in contravention to the order of the investigative judge or the State Prosecutor, the judgment may not be founded on the collected information. (2) Provisions of Article 211 paragraph 1, Article 293, paragraph 6, Article 356 paragraph 4, and Article 392 paragraph 4 of the present Code shall be applied accordingly with regard to the recordings made in breach of the provisions of this Article and Article 157 of the present Code. Article 162 of the CPC - Rendering Information to Persons Against Whom Measure of Secret Surveillance was Enforced when a Criminal Procedure is not Initiated (1) Before the material obtained through the enforcement of measures of secret surveillance in cases referred to in Article 160, paragraphs 4 and 5 of the present Code is destroyed, the investigative judge shall inform the person against whom the measure was undertaken, and that person shall have the right to examine the collected material. (2) If there is a reasonable concern that rendering information to the person referred to in paragraph 1 of this Article or examination of the collected material by such person could constitute a serious threat to the lives and health of people or could engender any investigation underway or if there are any other justifiable reasons, the investigative judge may, based on an opinion of the State Prosecutor, decide that the person against whom the measure was undertaken not be informed and allowed to examine the collected material. Article 15 - Conditions and safeguards Article 76 of the CPC - Search Warrant and Request for a Search Warrant 1 Each Party shall ensure that the establishment, implementation and 1) A search warrant shall be issued by the court at the request of the State application of the powers and procedures provided for in this Section are Prosecutor or at the request of an authorized police officer granted authorization subject to conditions and safequards provided for under its domestic law, by the State Prosecutor, and it shall be enforced by the police. which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the (2) A request for the issuance of a search warrant shall be submitted in writing, 1950 Council of Europe Convention for the Protection of Human Rights and and only exceptionally orally in line with Article 78 of the present Code.

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.

Article 83 of the CPC – Enteri Search Warrant and Searching

- 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.

DOMESTIC LEGISLATION

Article 83 of the CPC – Entering Another Person's Dwellings without a Search Warrant and Searching

- (1) An authorized police officer may enter another person's dwelling or other premises without a court order and, if necessary, carry out the search, if the tenant so requires or if somebody is seeking help or if it is necessary for the purpose of preventing the commission of a criminal offence or direct capturing of a criminal offender, or for the purpose of saving people and property, enforcement of a decision on detention or bringing in the accused person or other person, or for the purpose of deprivation of liberty of a criminal offence perpetrator who is on the run or a person from the arrest warrant, or if the search is to be carried out in public premises.
- (2) The tenant, if present, shall have the right to object to the procedure of the authorized police officer referred to in paragraph 1 of this Article. The authorized police officer shall inform the tenant about this right and shall include his/her objections in the receipt on entering the dwelling or in the search record.
- (3) In case referred to in paragraph 1 of this Article, if another person's dwelling was only entered without search, the tenant shall be issued a receipt stating the reason for entering the dwelling or other premises as well as the tenant's objections. If search was also carried out in another person's dwelling or other premises, the procedure shall be the one referred to in Article 81, paras. 3, 7 and 8 and Article 82, paragraph 1 of the present Code.
- (4) A search may also be carried out without the presence of witnesses if their presence during the search would expose the witnesses to risk of physical injuries or if it is not possible to arrange their presence immediately, and risk of delay exists. The reasons for the search without the presence of witnesses shall be specified in a record.
- (5) Authorized police employees may, without a search warrant and without the presence of witnesses, carry out a search of persons when enforcing a warrant on compulsory apprehension or when depriving of liberty, if suspicion exists that the person owns weapons or dangerous tools, or if suspicion exists that the person would reject, hide or destroy the objects that need to be taken from him/her as evidence in a criminal procedure.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (6) If there are grounds for suspicion that criminal offence was committed that is prosecuted by virtue of office, authorized police employees may, without a court warrant and without the presence of witnesses, carry out the search of transport means, passengers, luggage and other movable objects, with the exception of things referred to in Article 75 paragraph 2 of the present Code. (7) When conducting a search without a search warrant, authorized police officers shall immediately submit thereon a report to the investigative judge. Article 86 of the CPC - Denial of Disclosure or Issuing of Files 1) State authorities may refuse to disclose or issue their files and other documents if they deem that disclosure of their contents would cause damage to the public interests, with the exception of case of seizing the property gained through criminal activity. If disclosure or handover of files and other documents was denied, the final decision shall be made by the panel referred to in Article 24, paragraph 7 of the present Code. (2) Enterprises or other legal entities may request that data related to their business operations are not publicly disclosed. The panel referred to in Article 24 paragraph 7 of the present Code shall decide on the request. Article 16 - Expedited preservation of stored computer data Not specifically regulated in the CPC. 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 17 - Expedited preservation and partial disclosure of traffic data	Not specifically regulated in the CPC.
1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:	
a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and	
b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.	
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order	Not specifically regulated in the CPC.
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.	
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is	

DOMESTIC LEGISLATION

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:
- any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

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 computer system or part of it and computer data stored therein; and
- b a computer-data storage medium in which computer data may be stored

in its territory.

- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system (1) An authorized police officer may enter another person's dwelling or other 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:
- seize or similarly secure a computer system or part of it or a computer-data storage medium;
 - h make and retain a copy of those computer data;
 - maintain the integrity of the relevant stored computer data;
 - 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

Article 76 of the CPC - Search Warrant and Request for a Search Warrant

- 1) A search warrant shall be issued by the court at the request of the State Prosecutor or at the request of an authorized police officer granted authorization by the State Prosecutor, and it shall be enforced by the police.
- (2) A request for the issuance of a search warrant shall be submitted in writing, and only exceptionally orally in line with Article 78 of the present Code.

Article 83 of the CPC - Entering Another Person's Dwellings without a Search Warrant and Searching

- premises without a court order and, if necessary, carry out the search, if the tenant so requires or if somebody is seeking help or if it is necessary for the purpose of preventing the commission of a criminal offence or direct capturing of a criminal offender, or for the purpose of saving people and property, enforcement of a decision on detention or bringing in the accused person or other person, or for the purpose of deprivation of liberty of a criminal offence perpetrator who is on the run or a person from the arrest warrant, or if the search is to be carried out in public premises.
- (2) The tenant, if present, shall have the right to object to the procedure of the authorized police officer referred to in paragraph 1 of this Article. The authorized police officer shall inform the tenant about this right and shall include his/her objections in the receipt on entering the dwelling or in the search record.

DOMESTIC LEGISLATION

knowledge about the functioning of the computer system or measures applied (3) In case referred to in paragraph 1 of this Article, if another person's dwelling 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.

- was only entered without search, the tenant shall be issued a receipt stating the reason for entering the dwelling or other premises as well as the tenant's objections. If search was also carried out in another person's dwelling or other premises, the procedure shall be the one referred to in Article 81, paras. 3, 7 and 8 and Article 82, paragraph 1 of the present Code.
- (4) A search may also be carried out without the presence of witnesses if their presence during the search would expose the witnesses to risk of physical injuries or if it is not possible to arrange their presence immediately, and risk of delay exists. The reasons for the search without the presence of witnesses shall be specified in a record.
- (5) Authorized police employees may, without a search warrant and without the presence of witnesses, carry out a search of persons when enforcing a warrant on compulsory apprehension or when depriving of liberty, if suspicion exists that the person owns weapons or dangerous tools, or if suspicion exists that the person would reject, hide or destroy the objects that need to be taken from him/her as evidence in a criminal procedure.
- (6) If there are grounds for suspicion that criminal offence was committed that is prosecuted by virtue of office, authorized police employees may, without a court warrant and without the presence of witnesses, carry out the search of transport means, passengers, luggage and other movable objects, with the exception of things referred to in Article 75 paragraph 2 of the present Code.
- (7) When conducting a search without a search warrant, authorized police officers shall immediately submit thereon a report to the investigative judge.

Article 86 of the CPC – Denial of Disclosure or Issuing of Files

1) State authorities may refuse to disclose or issue their files and other documents if they deem that disclosure of their contents would cause damage to the public interests, with the exception of case of seizing the property gained through criminal activity. If disclosure or handover of files and other documents was denied, the final decision shall be made by the panel referred to in Article 24, paragraph 7 of the present Code.

Article 20 – Real-time collection of traffic data Art	Enterprises or other legal entities may request that data related to their siness operations are not publicly disclosed. The panel referred to in Article 24 ragraph 7 of the present Code shall decide on the request. ticle 157 of the CPC – Types of Secret Surveillance Measures and
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. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 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. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	If grounds for suspicion exist that a person has individually or in complicity the others committed, is committing or is preparing to commit criminal offences erred to in Article 158 of the present Code and evidence cannot be obtained in other manner or their obtaining would require a disproportional risk or dangering the lives of people, measures of secret surveillance may be ordered ainst those persons: Secret surveillance and recording of telephone conversations and other distance communication; Interception, collection and recording of computer data; Entry into premises for the purpose of secret photographing and video and audio recording in premises; Secret following and video and audio recording of persons and objects. If grounds for suspicion exist that a person has individually or in complicity the others committed, is committing or is preparing to commit criminal offences erred to in Article 158 of the present Code and circumstances of the case licate that evidence shall be collected with a minimum violation of the right to vacy, measures of secret surveillance may be ordered against those persons: Simulated purchase of objects or persons and simulated giving and taking of bribe; Providing simulated business services or concluding simulated legal transactions; Establishing fictitious companies; Supervision over the transportation and delivery of objects of criminal offence; Recording conversations upon previous informing and obtaining the consent of one of interlocutors; Hiring undercover investigators and collaborators.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	conveying to the perpetrator or from the perpetrator of criminal offences referred to in Article 158 of the present Code messages in connection to the criminal offence, or that the perpetrator has been using their telephone lines or other electronic communication devices.
	(4) In the case where there is no knowledge about the identity of the perpetrator of the criminal offence, the measures referred to in paragraph 1, item 4 of this Article may be ordered against the object of the criminal offence.
	(5) No criminal prosecution shall be undertaken against the persons who carry out the measures referred to in paragraph 2, items 1, 2, 5 and 6 of this Article, for acts which constitute aiding in committing a criminal offence, if it is done in order to provide information and evidence for the successful conduct of criminal proceedings.
	(6) Enforcement of measures referred to in paragraph 2, items 1, 2, 5 and 6 of this Article shall not constitute incitement to commit a criminal offence.
	(7) The measures referred to in paragraph 1, items 1 to 4 of this Article and measures referred to in paragraph 2, items 5 and 6 of this Article may be ordered against a person for whom an international arrest warrant was issued, or against a third party for whom there are grounds for suspicion that he is in direct contact with the person for whom there is an international arrest warrant.
	Article 158 of the CPC – Criminal Offences for Which Measures of Secret Surveillance May Be Ordered
	The measures referred to in Article 157 of the present Code may be ordered for the following criminal offences:
	1) for which a prison sentence of ten years or a more severe penalty may be imposed;
	2) having elements of organized crime;
	3) causing false bankruptcy, abuse of assessment, passive bribery, active bribery, trading in influence, abuse of an official position, as well as abuse of powers in economy, and fraud in the conduct of an official duty with prescribed imprisonment sentence of eight years or a more severe sentence;
	4) abduction, extortion, blackmail, meditation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful

BUDAPEST CONVENTION DOMESTIC LEGISLATION processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of evidences, criminal association, disclosure of confidential information, breach of confidentiality of proceedings, money laundering, counterfeiting of money, forgery of documents, falsification of official documents, making, procuring or providing to others means and materials for forging, participation in foreign armed formations, arranging outcomes of competitions., unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beings. 5) against the security of computer data. Article 159 of the CPC - Competence for Ordering Measures of Secret Surveillance and their Duration (1) Measures referred to in Article 157, paragraph 1 of the present Code shall be ordered via a written order by the investigative judge at the motion of the State Prosecutor containing a statement of reasons. The measures referred to in Article 157, paragraph 2 of the present Code shall be ordered by the State Prosecutor, at the reasoned motion of an authorized police officer or ex-officio, via a written order. The motion containing a statement of reasons shall be delivered in a closed envelope bearing the designation MSS - Measures of Secret Surveillance. (2) The motion and the order referred to in paragraph 1 of this Article shall contain: the type of measure, data on the person against whom the measure is enforced if this person is known, grounds for reasonable suspicion, the manner of measure enforcement, its goal, scope and duration. If it is a measure of engagement of an undercover agent and collaborator, the motion and the order shall also contain the use of false documents and technical devices for the transfer and recording of voice, image and video, participation in the conclusion of legal affairs, as well as the reasons justifying the engagement of a person who is not a police officer as an undercover agent and cooperative witness. (3) The motion and the order for ordering measures shall become an integral part of the criminal file and should contain available data on the person against whom they are ordered, the criminal offence because of which they are ordered, facts on basis of which the need to undertake them originates, duration deadline that needs to be suitable to achieving the objective of measure, manner, scope and

place for the measures to be implemented

BUDAPEST CONVENTION DOMESTIC LEGISLATION (4) By way of exception, if the written order cannot be issued in time and risk of delay exists, application of measure referred to in Article 157 of the present Code may begin on basis of a verbal order of the investigative judge, i.e., State Prosecutor. In that case, a written order must be obtained within 12 hours following the issue of the verbal order. (5) Based on the order of the investigating judge or State Prosecutor, the measures referred to in Article 157, paragraph 1 and paragraph 2, items 3 to 6 of the present Code may last up to four months. For justified reasons, these measures may be extended against the same person and for the same criminal offence no longer than 18 months from the adoption of the first order for imposing secret surveillance measures. Enforcement of the measures shall be terminated by an order when the reasons for their application cease. Measures whose enforcement was interrupted may continue for justified reasons against the same person and for the same criminal offence, based on an order. The maximum duration of the measure also includes the time during which the measure was interrupted. After the expiry of the periods referred to in this paragraph, enforcement of a measure may not continue, and new measures may not be ordered for the same criminal offence and against the same perpetrator. The motion for undertaking the measure referred to in Article 157, paragraph 2, items 1 and 2 of the present Code may refer only to one simulated act, and all subsequent motions for the application of this measure against the same person shall contain a statement of reasons justifying the repeated application of this measure. (6) If during the enforcement of the measure it shows out that the measure cannot achieve the intended purpose, it may be replaced by another measure. The maximum duration of the newly ordered measure shall include the duration of the previously ordered measures. (7) Ordering secret surveillance measures referred to in Article 157 para. 1 and 2 of the present Code against the same person and for the same criminal offence shall not affect the ordering of secret surveillance measures against a person for whom an international arrest warrant was issued or against a third party for whom there is reasonable suspicion that they are in direct contact with the person for whom there is an international arrest warrant. (8) In addition to the order for the application of measure referred to in Article

157, paragraph 1, item 1 of the present Code, the investigative judge shall issue

BUDAPEST CONVENTION DOMESTIC LEGISLATION a separate order containing solely the telephone number or e-mail address or the International Mobile Subscriber Identity (IMSI number), International Mobile Station Equipment Identity (IMEI number) and the internet protocol address (IP address) and the duration of the measure in question, and this order shall be delivered to enterprises referred to in paragraph 6 of this Article during the course of the application of the measure by the authorized police officers. (9) Postal agencies, other enterprises and legal entities registered for transmission of information shall enable the authorized police officers to enforce the measure referred to in Article 157, paragraph 1 of the present Code. Persons acting in an official capacity and responsible persons involved in the process of passing the order and enforcement of the measures referred to in Article 157 of the present Code shall keep as secret all the data they have learned in the course of this procedure. (10) If, during the enforcement of measures of secret surveillance, data and notifications are registered referring to some other persons for whom grounds for suspicion exist that s/he had committed the criminal offence for which a measure of secret surveillance was ordered, or some other criminal offence, that part of the material shall be copied and forwarded to the State Prosecutor, and it may be used as evidence only for criminal offences referred to in Article 158 of the present Code. (11) The State Prosecutor and the investigative judge shall, in an appropriate way (by coping records or official annotations without personal data, removal of an official annotation from the files and alike), prevent unauthorised persons, the suspects or their defence attorney to establish the identity of persons who have enforced the measures referred to in Article 157 of the present Code, as well as undercover agent and cooperative witness. If such persons are to be heard as witnesses, the court shall act in the manner prescribed in Articles 120-123 of the present Code. Article 160 of the CPC - Enforcement of Measures of Secret Surveillance (1) The measures referred to in Article 157 of the present Code shall be enforced by the authorized police officers in such a manner that the privacy of persons not subject to these measures be disturbed to the least extent possible. (2) Undercover agent and collaborator may be an authorized police officer,

employee in another public authority, authorized police officer of another state

BUDAPEST CONVENTION DOMESTIC LEGISLATION or, by way of exception, if the measure cannot be enforced in another manner, some other person. An undercover investigator shall be designated by the head of the body responsible for enforcement of secret surveillance measures or a person authorized by him. (3) Undercover agents and cooperative witnesses cannot be persons for whom reasonable suspicion exists that they were or that they currently are members of a criminal organization or group or persons who have been sentenced for criminal offences organized crime. (4) Undercover investigator and collaborator may participate in legal transactions by using false documents to conceal their identity, and when collecting information, they may use technical devices for the transfer and recording of sound, image and video. The body responsible for issuance of documents on the basis of which a person's identity may be established shall, at the request of the head of the body responsible for enforcement of secret surveillance measures, issue documents for concealing the identity of a police officer and other persons, entering into the database data from these documents. (5) Authorised police officer enforcing the measure shall keep records on each measure undertaken and report periodically to the State Prosecutor, that is, investigative judge on the enforcement of measures. If the State Prosecutor, i.e., investigative judge ascertains that the need for enforcement of the ordered measures does not exist anymore, s/he shall issue and order on their discontinuation. (6) Upon the enforcement of measures referred to in Article 157 of the present Code the authorized police officers shall submit to the State Prosecutor a final report and other material obtained by the enforcement of measures. (7) Should the State Prosecutor decide not to initiate a criminal procedure or if the data and information collected via secret surveillance measures are not necessary for the criminal proceedings, s/he shall forward to the investigative judge the material obtained through the application of Article 157 of the present Code, in a closed cover bearing the designation MSS, and the investigative judge shall order that the material be destroyed in the presence of the State Prosecutor and the investigative judge. The investigative judge shall compose a record thereon.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (8) The investigative judge shall proceed in the manner described in paragraph 7 of this Article if the State Prosecutor orders that investigation be conducted against the suspect who was subjected to measures of secret surveillance, when the results obtained or parts of the results are not indispensable for the conduct of the criminal proceedings or when the person for whom there is an international arrest warrant is found. (9) In cases referred to in paras. 7 and 8 of this Article, data shall be considered as classified within the meaning of regulation prescribing data secrecy. (10) The manner of production, use, keeping and destroying documents for establishing identity shall be governed by an act of the ministry responsible for internal affairs. **Article 161 of the CPC - Legally Invalid Evidence** (1) If the measures referred to in Article 157 of the present Code were undertaken in contravention to the provisions of the present Code or in contravention to the order of the investigative judge or the State Prosecutor, the judgment may not be founded on the collected information. (2) Provisions of Article 211 paragraph 1, Article 293, paragraph 6, Article 356 paragraph 4, and Article 392 paragraph 4 of the present Code shall be applied accordingly with regard to the recordings made in breach of the provisions of this Article and Article 157 of the present Code. Article 162 of the CPC - Rendering Information to Persons Against Whom Measure of Secret Surveillance was Enforced when a Criminal Procedure is not Initiated (1) Before the material obtained through the enforcement of measures of secret surveillance in cases referred to in Article 160, paragraphs 4 and 5 of the present Code is destroyed, the investigative judge shall inform the person against whom the measure was undertaken, and that person shall have the right to examine the collected material. (2) If there is a reasonable concern that rendering information to the person referred to in paragraph 1 of this Article or examination of the collected material by such person could constitute a serious threat to the lives and health of people

or could engender any investigation underway or if there are any other

DOMESTIC LEGISLATION

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:
- collect or record through the application of technical means on the territory of that Party, and
- compel a service provider, within its existing technical capability:

ito 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 15. Establishing fictitious companies; Articles 14 and 15.

justifiable reasons, the investigative judge may, based on an opinion of the State Prosecutor, decide that the person against whom the measure was undertaken not be informed and allowed to examine the collected material.

Article 157 of the CPC - Types of Secret Surveillance Measures and **Conditions for their Application**

- (1) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of the present Code and evidence cannot be obtained in another manner or their obtaining would require a disproportional risk or endangering the lives of people, measures of secret surveillance may be ordered against those persons:
- Secret surveillance and recording of telephone conversations and other distance communication;
- Interception, collection and recording of computer data;
- Entry into premises for the purpose of secret photographing and video and audio recording in premises;
- Secret following and video and audio recording of persons and objects.
- (2) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of the present Code and circumstances of the case indicate that evidence shall be collected with a minimum violation of the right to privacy, measures of secret surveillance may be ordered against those persons:
- 13. Simulated purchase of objects or persons and simulated giving and taking of bribe;
- 14. Providing simulated business services or concluding simulated legal transactions;
- 16. Supervision over the transportation and delivery of objects of criminal offence;
- 17. Recording conversations upon previous informing and obtaining the consent of one of interlocutors;
- 18. Hiring undercover investigators and collaborators.
- (3) Measures referred to in paragraph 1, item 1 of this Article may be also ordered against persons for whom there are grounds for suspicion that they have been

BUDAPEST CONVENTION DOMESTIC LEGISLATION conveying to the perpetrator or from the perpetrator of criminal offences referred to in Article 158 of the present Code messages in connection to the criminal offence, or that the perpetrator has been using their telephone lines or other electronic communication devices. (4) In the case where there is no knowledge about the identity of the perpetrator of the criminal offence, the measures referred to in paragraph 1, item 4 of this Article may be ordered against the object of the criminal offence. (5) No criminal prosecution shall be undertaken against the persons who carry out the measures referred to in paragraph 2, items 1, 2, 5 and 6 of this Article, for acts which constitute aiding in committing a criminal offence, if it is done in order to provide information and evidence for the successful conduct of criminal proceedings. (6) Enforcement of measures referred to in paragraph 2, items 1, 2, 5 and 6 of this Article shall not constitute incitement to commit a criminal offence. (7) The measures referred to in paragraph 1, items 1 to 4 of this Article and measures referred to in paragraph 2, items 5 and 6 of this Article may be ordered against a person for whom an international arrest warrant was issued, or against a third party for whom there are grounds for suspicion that he is in direct contact with the person for whom there is an international arrest warrant. Article 158 of the CPC - Criminal Offences for Which Measures of Secret **Surveillance May Be Ordered** The measures referred to in Article 157 of the present Code may be ordered for the following criminal offences: 1) for which a prison sentence of ten years or a more severe penalty may be imposed; 2) having elements of organized crime; 3) causing false bankruptcy, abuse of assessment, passive bribery, active bribery, trading in influence, abuse of an official position, as well as abuse of powers in economy, and fraud in the conduct of an official duty with prescribed imprisonment sentence of eight years or a more severe sentence; 4) abduction, extortion, blackmail, meditation in prostitution, displaying

pornographic material, usury, tax and contributions evasion, smuggling, unlawful

BUDAPEST CONVENTION DOMESTIC LEGISLATION processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of evidences, criminal association, disclosure of confidential information, breach of confidentiality of proceedings, money laundering, counterfeiting of money, forgery of documents, falsification of official documents, making, procuring or providing to others means and materials for forging, participation in foreign armed formations, arranging outcomes of competitions., unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beings. 5) against the security of computer data. Article 159 of the CPC - Competence for Ordering Measures of Secret **Surveillance and their Duration** (1) Measures referred to in Article 157, paragraph 1 of the present Code shall be ordered via a written order by the investigative judge at the motion of the State Prosecutor containing a statement of reasons. The measures referred to in Article 157, paragraph 2 of the present Code shall be ordered by the State Prosecutor, at the reasoned motion of an authorized police officer or ex-officio, via a written order. The motion containing a statement of reasons shall be delivered in a closed envelope bearing the designation MSS - Measures of Secret Surveillance. (2) The motion and the order referred to in paragraph 1 of this Article shall contain: the type of measure, data on the person against whom the measure is enforced if this person is known, grounds for reasonable suspicion, the manner of measure enforcement, its goal, scope and duration. If it is a measure of engagement of an undercover agent and collaborator, the motion and the order shall also contain the use of false documents and technical devices for the transfer and recording of voice, image and video, participation in the conclusion of legal affairs, as well as the reasons justifying the engagement of a person who is not a police officer as an undercover agent and cooperative witness. (3) The motion and the order for ordering measures shall become an integral part of the criminal file and should contain available data on the person against whom they are ordered, the criminal offence because of which they are ordered, facts on basis of which the need to undertake them originates, duration deadline that needs to be suitable to achieving the objective of measure, manner, scope and place for the measures to be implemented

DOMESTIC LEGISLATION

- (4) By way of exception, if the written order cannot be issued in time and risk of delay exists, application of measure referred to in Article 157 of the present Code may begin on basis of a verbal order of the investigative judge, i.e., State Prosecutor. In that case, a written order must be obtained within 12 hours following the issue of the verbal order.
- (5) Based on the order of the investigating judge or State Prosecutor, the measures referred to in Article 157, paragraph 1 and paragraph 2, items 3 to 6 of the present Code may last up to four months. For justified reasons, these measures may be extended against the same person and for the same criminal offence no longer than 18 months from the adoption of the first order for imposing secret surveillance measures. Enforcement of the measures shall be terminated by an order when the reasons for their application cease. Measures whose enforcement was interrupted may continue for justified reasons against the same person and for the same criminal offence, based on an order. The maximum duration of the measure also includes the time during which the measure was interrupted. After the expiry of the periods referred to in this paragraph, enforcement of a measure may not continue, and new measures may not be ordered for the same criminal offence and against the same perpetrator. The motion for undertaking the measure referred to in Article 157, paragraph 2, items 1 and 2 of the present Code may refer only to one simulated act, and all subsequent motions for the application of this measure against the same person shall contain a statement of reasons justifying the repeated application of this measure.
- (6) If during the enforcement of the measure it shows out that the measure cannot achieve the intended purpose, it may be replaced by another measure. The maximum duration of the newly ordered measure shall include the duration of the previously ordered measures.
- (7) Ordering secret surveillance measures referred to in Article 157 para. 1 and 2 of the present Code against the same person and for the same criminal offence shall not affect the ordering of secret surveillance measures against a person for whom an international arrest warrant was issued or against a third party for whom there is reasonable suspicion that they are in direct contact with the person for whom there is an international arrest warrant.
- (8) In addition to the order for the application of measure referred to in Article 157, paragraph 1, item 1 of the present Code, the investigative judge shall issue a separate order containing solely the telephone number or e-mail address or the

BUDAPEST CONVENTION DOMESTIC LEGISLATION International Mobile Subscriber Identity (IMSI number), International Mobile Station Equipment Identity (IMEI number) and the internet protocol address (IP address) and the duration of the measure in question, and this order shall be delivered to enterprises referred to in paragraph 6 of this Article during the course of the application of the measure by the authorized police officers. (9) Postal agencies, other enterprises and legal entities registered for transmission of information shall enable the authorized police officers to enforce the measure referred to in Article 157, paragraph 1 of the present Code. Persons acting in an official capacity and responsible persons involved in the process of passing the order and enforcement of the measures referred to in Article 157 of the present Code shall keep as secret all the data they have learned in the course of this procedure. (10) If, during the enforcement of measures of secret surveillance, data and notifications are registered referring to some other persons for whom grounds for suspicion exist that s/he had committed the criminal offence for which a measure of secret surveillance was ordered, or some other criminal offence, that part of the material shall be copied and forwarded to the State Prosecutor, and it may be used as evidence only for criminal offences referred to in Article 158 of the present Code. (11) The State Prosecutor and the investigative judge shall, in an appropriate way (by coping records or official annotations without personal data, removal of an official annotation from the files and alike), prevent unauthorised persons, the suspects or their defence attorney to establish the identity of persons who have enforced the measures referred to in Article 157 of the present Code, as well as undercover agent and cooperative witness. If such persons are to be heard as witnesses, the court shall act in the manner prescribed in Articles 120-123 of the present Code. Article 160 of the CPC - Enforcement of Measures of Secret Surveillance (1) The measures referred to in Article 157 of the present Code shall be enforced by the authorized police officers in such a manner that the privacy of persons not subject to these measures be disturbed to the least extent possible. (2) Undercover agent and collaborator may be an authorized police officer, employee in another public authority, authorized police officer of another state

or, by way of exception, if the measure cannot be enforced in another manner,

BUDAPEST CONVENTION DOMESTIC LEGISLATION

some other person. An undercover investigator shall be designated by the head of the body responsible for enforcement of secret surveillance measures or a person authorized by him.

- (3) Undercover agents and cooperative witnesses cannot be persons for whom reasonable suspicion exists that they were or that they currently are members of a criminal organization or group or persons who have been sentenced for criminal offences organized crime.
- (4) Undercover investigator and collaborator may participate in legal transactions by using false documents to conceal their identity, and when collecting information, they may use technical devices for the transfer and recording of sound, image and video. The body responsible for issuance of documents on the basis of which a person's identity may be established shall, at the request of the head of the body responsible for enforcement of secret surveillance measures, issue documents for concealing the identity of a police officer and other persons, entering into the database data from these documents.
- (5) Authorised police officer enforcing the measure shall keep records on each measure undertaken and report periodically to the State Prosecutor, that is, investigative judge on the enforcement of measures. If the State Prosecutor, i.e., investigative judge ascertains that the need for enforcement of the ordered measures does not exist anymore, s/he shall issue and order on their discontinuation.
- (6) Upon the enforcement of measures referred to in Article 157 of the present Code the authorized police officers shall submit to the State Prosecutor a final report and other material obtained by the enforcement of measures.
- (7) Should the State Prosecutor decide not to initiate a criminal procedure or if the data and information collected via secret surveillance measures are not necessary for the criminal proceedings, s/he shall forward to the investigative judge the material obtained through the application of Article 157 of the present Code, in a closed cover bearing the designation MSS, and the investigative judge shall order that the material be destroyed in the presence of the State Prosecutor and the investigative judge. The investigative judge shall compose a record thereon.
- (8) The investigative judge shall proceed in the manner described in paragraph 7 of this Article if the State Prosecutor orders that investigation be conducted against the suspect who was subjected to measures of secret surveillance, when

BUDAPEST CONVENTION DOMESTIC LEGISLATION the results obtained or parts of the results are not indispensable for the conduct of the criminal proceedings or when the person for whom there is an international arrest warrant is found. (9) In cases referred to in paras. 7 and 8 of this Article, data shall be considered as classified within the meaning of regulation prescribing data secrecy. (10) The manner of production, use, keeping and destroying documents for establishing identity shall be governed by an act of the ministry responsible for internal affairs. Article 161 of the CPC - Legally Invalid Evidence (1) If the measures referred to in Article 157 of the present Code were undertaken in contravention to the provisions of the present Code or in contravention to the order of the investigative judge or the State Prosecutor, the judgment may not be founded on the collected information. (2) Provisions of Article 211 paragraph 1, Article 293, paragraph 6, Article 356 paragraph 4, and Article 392 paragraph 4 of the present Code shall be applied accordingly with regard to the recordings made in breach of the provisions of this Article and Article 157 of the present Code. Article 162 of the CPC - Rendering Information to Persons Against Whom Measure of Secret Surveillance was Enforced when a Criminal Procedure is not Initiated (1) Before the material obtained through the enforcement of measures of secret surveillance in cases referred to in Article 160, paragraphs 4 and 5 of the present Code is destroyed, the investigative judge shall inform the person against whom the measure was undertaken, and that person shall have the right to examine the collected material. (2) If there is a reasonable concern that rendering information to the person referred to in paragraph 1 of this Article or examination of the collected material by such person could constitute a serious threat to the lives and health of people or could engender any investigation underway or if there are any other justifiable reasons, the investigative judge may, based on an opinion of the State Prosecutor, decide that the person against whom the measure was undertaken not be informed and allowed to examine the collected material.

DOMESTIC LEGISLATION

Section 3 - Jurisdiction

Article 22 - Jurisdiction

- Each Party shall adopt such legislative and other measures as may be Courts shall adjudicate within the limits of their subject matter jurisdiction necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
 - in its territory; or а
 - on board a ship flying the flag of that Party; or
 - on board an aircraft registered under the laws of that Party; or
 - 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.
- cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- Each Party shall adopt such measures as may be necessary to establish judges. 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.
- This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

established in accordance with this Convention, the Parties involved shall, jurisdiction for prosecution.

Article 23 of the CPC - Subject Matter Jurisdiction

prescribed by law.

Article 24 of the CPC - Composition of Court and Effective Court Jurisdiction

- (1) Courts shall adjudicate in the first instance in a panel composed of three judges with the exception of case referred to in paragraph 2 of this Article.
- (2) For criminal offences for which the prescribed principal punishment is a fine or imprisonment for a term of up to ten years, a single judge shall adjudicate in Each Party may reserve the right not to apply or to apply only in specific the first instance, with the exception of offences of the organized crime or unless otherwise prescribed by law.
 - (3) The second instance courts shall adjudicate in a panel composed of three
 - (4) The third instance courts shall adjudicate in a panel composed of five judges
 - (5) Preliminary investigation and investigation shall be participated by an investigative judge of a first instance court in line with this Code.
 - (6) The President of the Court and the Chair of the Panel shall decide in cases prescribed by the present Code.
- When more than one Party claims jurisdiction over an alleged offence (7) The first instance courts, adjudicating in a panel composed of three judges shall decide on appeals against rulings of the investigative judge and other rulings where appropriate, consult with a view to determining the most appropriate if so prescribed by the present Code, render decisions in the first instance out of main hearing, conduct the proceedings and render a verdict on the request for execution of a foreign court verdict, and make proposals in cases set forth in the present Code or other law.
 - (8) If the panel referred to in paragraph 7 of this Article cannot be established in a court adjudicating only in first instance due to an insufficient number of judges, affairs under the jurisdiction of that panel shall be conducted by the panel of immediately superior court.

BUDAPEST CONVENTION DOMESTIC LEGISLATION (9) Provisions of the present Code which refer to the rights and duties of the Chair of Panel and its members shall also be applied accordingly to an individual judge when s/he is adjudicating a case under the rules proscribed by the present Code. (10) When deciding on a motion for the protection of legality the court shall adjudicate in a panel composed of five judges. (11) Unless otherwise prescribed by the present Code, higher instance courts shall also adjudicate in a panel composed of three judges when deciding cases not specified in paras. 3, 4 and 10 of this Article. Article 25 of the CPC – General Rules of Determining Territorial Jurisdiction (1) As a rule, the court within whose territory criminal offence was committed or attempted shall have the territorial jurisdiction. (2) A private action may be filed with the court within the territory of which the accused person has a permanent or a temporary residence. (3) If the criminal offence was committed or attempted within the territory of several courts or on the border of those territories, or if it is uncertain within which territory the offence has been committed or attempted, the court which on the indictment of the authorized prosecutor has first instituted the procedure shall have jurisdiction, whereas in preliminary investigation and investigation the competent court is the one that was the first to undertake an action on basis of the prosecutor's motion. Article 26 of the CPC - Territorial Jurisdiction of Courts in Cases of Offences Committed on a National Vessel or Aircraft If an offence was committed on a national vessel or aircraft while it was in a home port or airport, the competent court shall be the one whose territory includes that port or airport. In other cases where a criminal offence has been committed on a national vessel or aircraft, the competent court shall be the court whose territory includes the home port of the vessel or home airport of the aircraft or domestic port or airport where the vessel or aircraft first time stops. Article 27 of the CPC - Territorial Jurisdiction for an Offence Committed by Means of Media

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) If a criminal offence is committed by means of press, the competent court shall be the one within whose territory the newspaper was printed. If this location is unknown or if the newspaper was printed abroad, the competent court shall be the one within whose territory printed newspaper is distributed.
	(2) If according to law the compiler of the text is responsible, the competent court shall be the one within whose territory the compiler has permanent residence or the court within whose territory the event to which the text refers to took place.
	(3) Provisions of paras. 1 and 2 of this Article shall also be applied accordingly to cases where the statement or text was released by radio, television or other mass media.
	Article 28 of the CPC – Territorial Jurisdiction in Cases When the Place of Commission of a Criminal Offence is Unknown
	(1) If the place of the commission of a criminal offence is unknown or if this place is not in the territory of Montenegro, the competent court shall be the one within whose territory the accused person has temporary or permanent residence.
	(2) If the procedure is already pending before the court of the accused person's temporary or permanent residence, when the place of the commission has been determined, this court shall retain its jurisdiction.
	(3) If neither the place of the commission of the criminal offence nor the temporary or permanent residence of the accused person is known, or if both of them are outside the territory of Montenegro, the competent court shall be the one within whose territory the accused person is deprived of liberty or turned himself/herself in.
	Article 29 of the CPC – Territorial Jurisdiction in Cases of Criminal Offences Committed in Montenegro and Abroad
	If a person has committed a criminal offence both in Montenegro and abroad, the competent court shall be the one that has jurisdiction over the criminal offence committed in Montenegro.

DOMESTIC LEGISLATION

Article 30 of the CPC – Set Territorial Jurisdiction (Forum Ordinatum)

If under the provisions of the present Code it is not possible to ascertain which court has territorial jurisdiction, the Supreme Court of Montenegro (hereinafter: the Supreme Court) shall designate one of the competent courts as to subject matter jurisdiction to conduct the proceedings.

Chapter III - International co-operation

Article 24 - Extradition

- 1 a This article applies to extradition between Parties for the criminal Article 10 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.
- Where a different minimum penalty is to be applied under an Article 11 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 5. 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.

Law on International Legal Assistance in Criminal Matters

The extradition of the accused or sentenced persons shall be requested and enforced in accordance with this Law unless otherwise has been provided for under an international agreement.

- (1) The conditions for the extradition upon the request of the Requesting State shall be as follows:
- 1. that the person claimed is not a national of Montenegro;
- 2. that the offence for which extradition is requested was not committed in the territory of Montenegro, against Montenegro or its national;
- 3. that the offence motivating the request for extradition is a criminal offence both under the domestic law and under the law of the country in which it was committed:
- 4. that the criminal prosecution or enforcement of criminal sanction has not been barred by the lapse of time under the domestic law before the person claimed has been detained or examined as an accused:
- that the person claimed has not been already convicted by a domestic court for the same offence or he has not been acquitted of the same offence by the domestic court in a final and legally binding manner, except if the requirements prescribed by the Criminal Procedure Code for retrial have been met; or criminal proceedings have not been instituted in Montenegro for the same offence committed against Montenegro or a national of Montenegro; or the security for the fulfilment of property law claim of the victim has been

- 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
- 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.
- 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
- b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure

DOMESTIC LEGISLATION

- provided if the proceedings have been instituted for the offence committed against a national of Montenegro:
- 6. that the identity of the person claimed has been established;
- that the requesting state presented facts and sufficient evidence for a grounded suspicion that the person claimed committed the criminal offence or there is a final and legally binding judicial decision.

Article 12

- (1) The extradition shall not be allowed for a political criminal offence, an offence connected with a political criminal offence or a military criminal offence within the meaning of the European Convention of Extradition (hereinafter referred to as "political and military criminal offences").
- (2) Prohibition referred to in paragraph 1 above shall not apply to the criminal offences of genocide, crime against humanity, war crimes and terrorism.

Article 25 - General principles relating to mutual assistance

- 1 The Parties shall afford one another mutual assistance to the widest extent | Article 3 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 by this law. 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

Law on International Legal Assistance in Criminal Matters

Mutual legal assistance shall include the extradition of the accused and sentenced persons, transfer and assuming of criminal prosecution, enforcement of foreign criminal verdicts, as well as other forms of mutual legal assistance provided for

Article 4

(1) Domestic judicial authority shall forward letters rogatory for mutual legal assistance to foreign judicial authorities and receive the letters rogatory for mutual legal assistance of the foreign judicial authorities through the ministry responsible for the judiciary (hereinafter referred to as the "Ministry").

to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual requested Party or by applicable mutual assistance treaties, including the 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 deliver copy of letter rogatory to the Ministry. request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

DOMESTIC LEGISLATION

- required by the requested Party. The requested Party shall accept and respond (2) In cases where there is no international agreement or reciprocity, the Ministry shall deliver and receive letters rogatory for mutual legal assistance through diplomatic channels.
- assistance shall be subject to the conditions provided for by the law of the (3) Exceptionally, in cases when provided for under an international agreement or where there is reciprocity, the national judicial authority may deliver directly grounds on which the requested Party may refuse co-operation. The requested or indirectly to the competent foreign judicial authority and receive letters rogatory for mutual legal assistance of the foreign state, with the obligation to
 - (4) In urgent cases, provided that there is reciprocity, letter rogatory for mutual legal assistance may be delivered and received through the National Central Bureau of the Interpol.
 - (5) The courts and the state prosecutors' offices shall be responsible for provision of mutual legal assistance in accordance with the law.

Article 5

Mutual criminal assistance may be provided if the offence for which the provision of i mutual legal assistance is requested is a criminal offence both under the domestic law and under the law of the foreign state the judicial authority of which presented the letter rogatory for mutual legal assistance.

Article 5a

- (1) Should the competent authority of the Requesting State require confidential treatment, letter rogatory may only be made available to the competent authorities to act on it and to the extent necessary for the procedure.
- (2) Should the confidentiality under paragraph 1 not be possible, the Ministry or national judicial authority shall inform the competent authority of the Requesting State.
- (3) Personal data received in response to the letter rogatory can only be used for the purpose of the proceedings for which required, as well as other legal proceedings connected with that process.

Article 6

(1) Unless otherwise has been provided for by an international agreement or this Law, the letter rogatory for mutual legal assistance of the domestic or of the

BUDAPEST CONVENTION DOMESTIC LEGISLATION

foreign judicial authority shall be accompanied with the translation of the letter rogatory into the language of the requested state, or one of the official languages of the Council of Europe, if the requested state accepts it. The replies to the letters rogatory of the foreign judicial authorities do not need to be translated.

(2) Domestic judicial authority shall also proceed upon the letter rogatory for mutual legal assistance of the foreign judicial authority if the letter rogatory has been presented electronically or by some other means of telecommunication providing delivery receipt, if it may verify its authenticity and if the foreign judicial authority is prepared to deliver the original of the letter rogatory within 15 days at latest.

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.

Law on International Legal Assistance in Criminal Matters in the absence of applicable international agreements.

Article 27 - Procedures pertaining to mutual assistance requests in Article 4 of the Law on mutual legal assistance in criminal matters the absence of applicable international agreements

- 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 responsible for the judiciary (hereinafter referred to as the "Ministry"). or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- Each Party shall designate a central authority or authorities responsible diplomatic channels. for sending and answering requests for mutual assistance, the execution of

(Official Gazette of Montenegro, no. 04/2008 and 36/2013)

- 1 Where there is no mutual assistance treaty or arrangement on the basis of (1) Domestic judicial authority shall forward letters rogatory for mutual legal uniform or reciprocal legislation in force between the requesting and requested assistance to foreign judicial authorities and receive the letters rogatory for mutual legal assistance of the foreign judicial authorities through the ministry
 - (2) In cases where there is no international agreement or reciprocity, the Ministry shall deliver and receive letters rogatory for mutual legal assistance through

execution.

- The central authorities shall communicate directly with each other;
- 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;
- 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.
- 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.
- The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
- the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
- The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
- 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.
- 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.

DOMESTIC LEGISLATION

- such requests or their transmission to the authorities competent for their (3) Exceptionally, in cases when provided for under an international agreement or where there is reciprocity, the national judicial authority may deliver directly or indirectly to the competent foreign judicial authority and receive letters rogatory for mutual legal assistance of the foreign state, with the obligation to deliver copy of letter rogatory to the Ministry.
 - (4) In urgent cases, provided that there is reciprocity, letter rogatory for mutual legal assistance may be delivered and received through the National Central Bureau of the Interpol.
 - (5) The courts and the state prosecutors' offices shall be responsible for provision of mutual legal assistance in accordance with the law.

DOMESTIC LEGISLATION

- 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
- b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
- c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
- d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
- e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 - Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

Law on International Legal Assistance in Criminal Matters in the absence of applicable international agreements.

BUDAPEST CONVENTION DOMESTIC LEGISLATION 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material. Law on International Legal Assistance in Criminal Matters in the Article 29 - Expedited preservation of stored computer data absence of applicable international agreements. 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. A request for preservation made under paragraph 1 shall specify: the authority seeking the preservation; the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; the stored computer data to be preserved and its relationship to the offence: any available information identifying the custodian of the stored computer data or the location of the computer system; the necessity of the preservation; and 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. Upon receiving the request from another Party, the requested Party

shall take all appropriate measures to preserve expeditiously the specified

BUDAPEST CONVENTION DOMESTIC LEGISLATION 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. 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. In addition, a request for preservation may only be refused if: the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request. Article 30 - Expedited disclosure of preserved traffic data Law on International Legal Assistance in Criminal Matters in the absence of applicable international agreements. 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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
that service provider and the path through which the communication was transmitted.	
2 Disclosure of traffic data under paragraph 1 may only be withheld if:	
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or	
b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data	International legal assistance in cases related to cybercrime is currently realized through the National Office of Interpol in Podgorica.
1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.	
2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.	
3 The request shall be responded to on an expedited basis where:	
a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or	
b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available	International legal assistance in cases related to cybercrime is currently realized through the National Office of Interpol in Podgorica.
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.	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 - Mutual assistance regarding the interception of content data	International legal assistance in cases related to cybercrime is currently realized through the National Office of Interpol in Podgorica.
The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network	
1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:	
a the provision of technical advice;	
b the preservation of data pursuant to Articles 29 and 30;	
c the collection of evidence, the provision of legal information, and locating of suspects.	
2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.	
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	

DOMESTIC LEGISLATION

extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Article 42 - Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its In accordance with Article 9, paragraph 4, and with regard to Article 9, paragraph 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Reservation contained in the instrument of ratification deposited on 3 March 2010 - Or. Engl.

instrument of ratification, acceptance, approval or accession, declare that it 1, item e, of the Convention, Montenegro declares that obtaining child avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article pornography through computer systems for oneself and other persons and possession of child pornography in computer systems or on mediums for storage of computer data shall not be considered offences in case the person displayed in these materials turned fourteen years of age and gave his/her consent.

> Reservation contained in the instrument of ratification deposited on 3 March 2010 - Or. Engl.

> In accordance with Article 9, paragraph 4, and with regard to Article 9, paragraph 2, item b, of the Convention, Montenegro declares that materials which visually display face by which it can be concluded that the person is a minor engaged in an explicit act as stated in Article 9, paragraph 2, item b, of this Convention shall not be considered child pornography.

> Reservation contained in the instrument of ratification deposited on 3 March 2010 - Or. Engl.

> In accordance with Article 14, paragraph 3, and with regard to Article 20, of the Convention, Montenegro declares that measures from Article 20 of the Convention shall be applied solely on the basis of the decision of a competent Montenegrin court, if it is necessary for conducting a criminal procedure or for reasons of safety in Montenegro.