Moldova

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Law on preventing and combating cybercrime, nr. 20-XVI, 03.02.2009** **Article 2 - The main notions** **computer system** – any device or group of devices isolated interconnected or related providing times of which one or more elements, pursuant to a programme, automatic processing of data; **computer information**-any representation of facts, information or concepts in a form suitable for processing in an information system, including a program capable of executing a function performed by a computer system; **service provider** shall mean any public or private entity that offers its users the ability to communicate by means of a computer system, and any other entity that processes or stores computer data communications for this service or to its users; **traffic data** – data having any connection with a communication submitted by a computer system, products of this system as an element of the chain of communication, indicating origin, destination, route, time, date, size, duration, or type of underlying service; **Security measures** – procedures, specialized software or devices that access to a computer system is restricted or banned for certain categories of users.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Article 259. Illegal Access to Computerized Information** (1) Illegal access to computerized information meaning the data from computers, data storage devices, computer systems, or networks by a person unauthorized by law or contract or who exceeds the limits of his/her authorization or who does not have permission from a competent person to use, administer, or control a data system or to conduct scientific research or to perform any other operation in a data system, provided that such access is accompanied by destroying, deteriorating, changing, blocking or copying information, the malfunction of the computers, computer systems or networks, and provided that such access causes large-scale damage shall be punished by a fine in the amount of 200 to 500 conventional units or by community service for 150 to 200 hours or by imprisonment for up to 2 years, whereas a legal entity shall be punished by a fine in the amount of 1000 to 3000 conventional units with the deprivation of the right to practice certain activities. (2) The same action committed: *[Letter a) excluded by Law No. 277-XVI dated 18.12.2008, in force as of 24.05.2009]* b) by two or more persons; c) by breaching protection systems; d) via connection to telecommunication channels; e) with the use of special technical means; f) with the illegal use of the computer, computer system, or network in order to commit one of the crimes set forth in par. (1) of art. 2601-2603, 2605 and 2606; g) in respect to information protected by law; h) on an especially large scale; 116 shall be punished by a fine in the amount of 500 to 1000 conventional units or community service for 180 to 240 hours or by imprisonment for up to 3 years, whereas a legal entity shall be punished by a fine in the amount of 3000 to 6000 conventional units with the deprivation of the right to practice certain activities or by the liquidation of the legal entity. *[Art.259 amended by Law No. 277-XVI dated 18.12.2008, in force as of*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	24.05.2009] *[Art.259 amended by Law No. 278-XVI dated 18.12.2008, in force as of 20.02.2009]* *[Art.259 amended by Law No. 184-XVI dated 29.06.2006, in force as of 11.08.2006]* *[Art.259 completed by Law No. 211-XV dated 29.05.03, in force as of 12.06.03]*
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Article 260[1]. Illegal Interception of an Information Data Transfer** The illegal interception of an information data transfer (including an electronic emission) that are not public and are intended for the data system, that originate from such a system or are performed within a data system shall be punished by a fine in the amount of 500 to 1000 conventional units or by imprisonment for 2 to 5 years, whereas a legal entity shall be punished by a fine in the amount of 3000 to 6000 conventional units with the deprivation of the right to practice certain activities or by the liquidation of the legal entity. *[Art.2601 introduced by Law No. 278-XVI dated 18.12.2008, in force as of 20.02.2009]*
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Article 260[2]. Violation of the Integrity of the Information Data Contained in a Data System** The deliberate modification, deletion, or damaging of information data contained in a data system or the illegal restriction of access to such data or the unauthorized transfer of information data from a data system or a storage device or obtaining, marketing, or offering in any form of information data with limited access provided that such actions cause large-scale damage shall be punished by a fine in the amount of 500 to 1000 conventional units or by imprisonment for 2 to 5 years. *[Art.2602 introduced by Law No. 278-XVI dated 18.12.2008, in force as of 20.02.2009]*
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Article 260[3]. Impact on Data System Operation** (1) Impact on a data system's operation by introducing, transmitting, modifying, deleting or deteriorating information data or by limiting access to such data provided that such actions cause large-scale damage shall be punished by a fine in the amount of 700 to 1000 117 conventional units or by community service for 150 to 200 hours or by imprisonment for 2 to 5 years, whereas a legal entity shall be punished by a fine in the amount of 3000 to 6000 conventional units with the deprivation of the right to practice certain activities or by the liquidation of the legal entity.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) The same action: a) committed for material interests; b) committed by two or more persons; c) committed by an organized criminal group or a criminal organization; d) causing damage on an especially large scale; shall be punished by a fine in the amount of 700 to 1000 conventional units or by imprisonment for 3 to 7 years, whereas a legal entity shall be punished by a fine in the amount of 3000 to 6000 conventional units or by the liquidation of the legal entity. *[Art.260³ introduced by Law No. 278-XVI dated 18.12.2008, in force as of 20.02.2009]*
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or	**Article 260. Illegal Production, Importation, Marketing, or Offering of Technical Means or Software Products** (1) The production, importation, marketing or otherwise offering in an illegal manner of technical means or software products developed or adapted in order to commit one of crimes set forth in art. 237, 259, 2601-2603, 2605 and 2606 shall be punished by a fine in the amount of 500 to 1000 conventional units or by imprisonment for 2 to 5 years, whereas a legal entity shall be punished by a fine in the amount of 3000 to 6000 conventional units with the deprivation of the right to practice certain activities or by the liquidation of the legal entity. *[Art.260 in version of Law No. 278-XVI dated 18.12.2008, in force as of 20.02.2009]* *[Art.260 amended by Law No. 184-XVI dated 29.06.2006, in force as of 11.08.2006]* *[Art.260 completed by Law No. 211-XV dated 29.05.03, in force as of 12.06.03]*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 260[5]. Information Data Forgery** The illegal introduction, change, or deletion of information data or the illegal limitation of access to such data generating unauthentic data to be used for the production of a legal consequence shall be punished by a fine in the amount of 1000 to 1500 conventional units or by imprisonment for 2 to 5 years. *[Art.2605 introduced by Law No. 278-XVI dated 18.12.2008, in force as of 20.02.2009]*
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Article 260[6]. Information Fraud** 118 (1) Introducing, changing, or deleting information data, limiting access to such data, or in any way preventing a data system's operation in order to gain material benefit either personal or for another person provided that such actions caused large-scale damage shall be punished by a fine in the amount of 1000 to 1500 conventional units or by community service for 150 to 200 hours or by imprisonment for 2 to 5 years. (2) The same actions: a) committed by an organized criminal group or a criminal organization; b) causing damage on an especially large scale; shall be punished by imprisonment for 4 to 9 years. *[Art.2606 introduced by Law No. 278-XVI dated 18.12.2008, in force as of 20.02.2009]*
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	**Article 208[1]. Infantile Pornography** The production, distribution, broadcasting, import, export, offering, sale, exchange, use, or holding of pictures or of other images of one or more children

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	involved in explicit, real, or simulated sexual activities or pictures or other images of genital organs of a child represented in a lustful or indecent manner including in a soft version shall be punished by imprisonment for 1 to 3 years whereas a legal entity shall be punished by a fine in the amount of 2000 to 4000 conventional units with the deprivation of the right to practice certain activities. *[Art.2081 introduced by Law No. 235-XVI dated 08.11.2007, in force as of 07.12.2007]*
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property	**Art. 185[1]. Violation of Copyright and Associated Rights** (1) Assuming an author's rights (plagiarism) or any other violation of copyright and/or associated rights if the value of the rights infringed or the value of the licensed work, software, database, performance, logo or broadcasts that are the object of a copyright or associated rights is large scale and when such an assumption is committed by: a) reproducing, in whole or in part, the work protected by copyright or associated rights;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	b) the sale, rental, import, export, transport, storage, or publication of the work protected by copyright or associated rights; c) the public broadcasting of a cinematographic work or of an audio-visual work via radio/electronic means or cable in an interactive mode, including via Internet or another similar procedure; d) public broadcasting of the original work or of a copy; e) public performance of the work; f) simultaneous or subsequent rebroadcast of the work, performance, or program via radio/electronic means or cable or by another similar procedure or in places with a paid entry; g) recording of the audio-visual work, program, or performance in concert halls, cinemas, and in another public places without the consent of the holder of rights over the work, program, or performance; h) allowing public access to a computer database that contains or constitutes work protected by copyright; i) translation, publication in editions, adaptation or transformation of work, and the processing and arrangement thereof; shall be punished by a fine in the amount of 800 to 1000 conventional units or by community service for 180 to 240 hours, whereas a legal entity shall be punished by a fine in the amount of 2000 to 4000 conventional units with the deprivation of the right to practice certain activities for 1 to 5 years. 77 (2) The sale, rental, or exchange of copies of works infringing copyright or associated rights by public announcements, via means of electronic communication, or through public displays of catalogues with covers or of covers of works or logos, the deliberate allocation by legal entities of their own spaces, equipment, means of transport, goods or services for the purpose of illegal use by another individual or legal entity of works and/or performances, logos, or programs that are the object of copyright or associated rights, as well as a refusal to declare the origin of the copies or logos sold, rented, or exchanged infringing copyright or associated rights shall be punished by a fine in the amount of 800 to 1000 conventional units or by community service for 180 to 240 hours, whereas a legal entity shall be punished by a fine in the amount of 2000 to 4000 conventional units with the deprivation of the right to practice

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	certain activities for 1 to 5 years. (3) The sale, rental, exchange, free transmission, export, storage, or other use of copies of works and/or logos, software, or databases without relevant trademarks and without having, at the time of control, copyright agreements signed with the holders of rights over the aforementioned objects, as well as the improper application of trademarks, other than those applied on material objects specified in the annexes to the request for issuing trademarks or the application of trademarks on copies or logos without the consent of the copyright holder, provided that the value of such objects is large scale, shall be punished by a fine in the amount of 800 to 1000 conventional units or by community service for 180 to 240 hours, whereas a legal entity shall be punished by a fine in the amount of 2000 to 4000 conventional units with the deprivation of the right to practice certain activities for 1 to 5 years. (4) Avoiding by technical means used for the protection of copyright and associated rights as well as the removal or change of information on the management of copyright and other associated rights, irrespective of whether these rights were violated or not, shall be punished by a fine in the amount of 800 to 1000 conventional units or by community service for 180 to 240 hours, whereas a legal entity shall be punished by a fine in the amount of 2000 to 4000 conventional units with the deprivation of the right to practice certain activities for 1 to 5 years. (5) The illegal marking, sale, import, export, transport, or storage of trademarks and the falsification thereof causing large-scale damage shall be punished by a fine in the amount of 2000 to 4000 conventional units or by community service for 180 to 240 hours, whereas a legal entity shall be punished by a fine in the amount of 2000 to 6000 conventional units with the deprivation of the right to practice certain activities for 1 to 5 years. (6) The actions set forth in par. (1), (2), (3), (4) or (5) committed: *[Letter a) excluded by Law No. 277-XVI dated 18.12.2008, in force as of 24.05.2009]* b) by two or more persons; c) by an organized criminal group or by a criminal organization; d) through physical or mental coercion; e) on an especially large scale; shall be punished by a fine in the amount of 4000 to 5000 conventional units or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	by imprisonment for 3 to 5 years, whereas a legal entity shall be punished by a fine in the amount of 8000 to 10,000 conventional units with the deprivation of the right to practice certain activities for 1 to 5 years or by the liquidation of the legal entity. *[Art.185¹ amended by Law No. 110-XVI dated 27.04.2007, in force as of 08.06.2007]* *[Art.185¹ introduced by Law No. 446-XV dated 30.12.04, in force as of 28.01.05]*
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural	**Art.21. Subject of the Crime** (3) A legal entity, except for public authorities, shall be subject to criminal liability for an act set forth in criminal law provided that one of the following conditions is applicable: a) the legal entity is guilty of failure to comply or improper compliance with direct legal provisions defining obligations or prohibitions to perform a certain activity; 19 b) the legal entity is guilty of carrying out an activity that does not comply with its founding documents or its declared goals; c) the act causes or threatens to cause considerable damage to a person to society, or to the state and was committed for the benefit of this legal entity or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	was allowed, sanctioned, approved, or used by the body or the person empowered with the legal entity's administrative functions. (4) Legal entities, except for public authorities, shall be criminally liable for crimes punishable in line with the special part of this Code applicable to legal entities. (5) The criminal liability of a legal entity does not exclude the liability of the individual for the crime committed. *[Art.21 amended by Law No. 277-XVI dated 18.12.2008, in force as of 24.05.2009]* *[Art.21 completed by Law No.181-XVI dated 10.07.2008, in force as of 01.11.2008]* *[Art.21 amended by Law No..136-XVI dated 19.06.2008, in force as of 08.08.2008]* *[Art.21 completed by Law No.235-XVI dated 08.11.2007, in force as of 07.12.2007]* *[Art.21 amended by Law No.110-XVI dated 27.04.2007, in force as of 08.06.2007]* *[Art.21 completed by Law No.30-XVI dated 23.02.06, in force as of 17.03.06]* *[Art.21 amended by Law No.376-XVI dated 29.12.05, in force as of 31.01.06]* *[Art.21 amended by Law No.277-XVI dated 04.11.05, in force as of 02.12.05]* *[Art.21 completed by Law No.446-XV dated 30.12.04, in force as of 28.01.05]* *[Art.21 completed by Law No.158-XV dated 20.05.04, in force as of 18.06.04]* *[Art.21 amended by Law No.305-XV dated 11.07.03, in force as of 22.07.03]* *[Art.21 amended by Law No.211-XV dated 29.05.03, in force as of 12.06.03]*
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	***See below for implementation of specific procedural powers***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	**Law on preventing and combating cybercrime, nr. 20-XVI, 03.02.2009** **Article 3. The basic principles of prevention and fight against cybercrime** Preventing and combating cybercrime is carried out on the following principles: a) legality; b) respect for human rights and fundamental freedoms; c) promptness; d the inevitability of punishment); e-crime and security protection) personal data; f) use complex measures of prevention: legal, socio-economic and information technology; g) social partnership, cooperation between public administration authorities with international organizations, non-governmental organizations, other civil society representatives.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.	**Law on preventing and combating cybercrime, nr. 20-XVI, 03.02.2009** **Article 6. Obligations of owners of systems computer** 7. The obligations of service providers (1) service providers are obliged: c) to carry out, under conditions of confidentiality, the competent authority on request the immediate preservation of computer data or computer data related to trafficking, to which there is a danger of destruction or alteration, for a period of up to 120 calendar days in accordance with national legislation; g) ensure the deciphering of computer data that is contained in the packages with network protocols to preserve such data for a period of at least 90 calendar days. **Article 7. Obligations of service providers** (1) Service providers are obliged:

Back to the Table of Contents

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.	a) to keep records of service users; b) to notify the competent authorities about the web traffic data, including the data about illegal access to computer system information, about the attempts to introduce illegal programs, about the violation by competent persons of the rules of collection, processing, storage, transmission and distribution of information or of rules of computer system protection provided according to the information importance or to its degree of protection, if they have contributed to acquisition, distortion or destruction of information or if they have caused other serious consequences, perturbation of computer systems functioning and other computer crimes; c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of web traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation; d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user; e) to undertake security measures by means of using some procedures, devices or specialized computer programs, with the help of which to restrict or forbid the unauthorized users to access a computer system; f) to ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted g) to ensure the interpretation of computer data from network protocols packages, preserving such data for a period of at least 90 calendar days. (2) If the web traffic data are possessed by several service providers, then the requested service provider is obliged to submit to the competent authority the necessary information for the identification of the other service providers.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available	**Law on preventing and combating cybercrime, nr. 20-XVI, 03.02.2009** **Article 6. Obligations of owners of systems computer** 7. The obligations of service providers (1) service providers are obliged

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	d) to submit to the competent authorities, pursuant to a request made in accordance with the law, data relating to users, including the type of communication and service to the user, the method of payment of the service, and any other data which may lead to the identification of the user; (2) where data on traffic data is in possession of several service providers, called service provider is obliged to immediately provide the competent authority with the information necessary to identify other suppliers of services. Article 7. Obligations of service providers (1) Service providers are obliged: a) to keep records of service users; b) to notify the competent authorities about the web traffic data, including the data about illegal access to computer system information, about the attempts to introduce illegal programs, about the violation by competent persons of the rules of collection, processing, storage, transmission and distribution of information or of rules of computer system protection provided according to the information importance or to its degree of protection, if they have contributed to acquisition, distortion or destruction of information or if they have caused other serious consequences, perturbation of computer systems functioning and other computer crimes; c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of web traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation; d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user; e) to undertake security measures by means of using some procedures, devices or specialized computer programs, with the help of which to restrict or forbid the unauthorized users to access a computer system; f) to ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	transmitted g) to ensure the interpretation of computer data from network protocols packages, preserving such data for a period of at least 90 calendar days. (2) If the web traffic data are possessed by several service providers, then the requested service provider is obliged to submit to the competent authority the necessary information for the identification of the other service providers.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**Law on preventing and combating cybercrime, nr. 20-XVI, 03.02.2009** **Article 5. Cooperation of the competent authorities in Prevention of and fight against cybercrime** Within the framework of the activities of prevention and cybercrime, the competent authorities, service providers, non-governmental organizations, other civil society representatives shall collaborate through information exchange, expert, through joint research activities of cases and identification of offenders, staff training, by developing initiatives to promote programs, best practices, measures, procedures and minimum standards of security of computer systems through information campaigns on cybercrime and the risks to which they are exposed to users of computer systems through other activities in this field. **Article 7. Obligations of service providers** (1) Service providers are obliged: a) to keep records of service users; b) to notify the competent authorities about the web traffic data, including the data about illegal access to computer system information, about the attempts to introduce illegal programs, about the violation by competent persons of the rules of collection, processing, storage, transmission and distribution of information or of rules of computer system protection provided according to the information importance or to its degree of protection, if they have contributed to acquisition, distortion or destruction of information or if they have caused other serious consequences, perturbation of computer systems functioning and other computer crimes; c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of web traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	provisions of national legislation; d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user; e) to undertake security measures by means of using some procedures, devices or specialized computer programs, with the help of which to restrict or forbid the unauthorized users to access a computer system; f) to ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted g) to ensure the interpretation of computer data from network protocols packages, preserving such data for a period of at least 90 calendar days. (2) If the web traffic data are possessed by several service providers, then the requested service provider is obliged to submit to the competent authority the necessary information for the identification of the other service providers.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures	**Article 125. Grounds for conducting a search** (1) The criminal prosecution body has the right to make a search if the collected evidence or evidence collected in the on going investigation justly presuppose that in a certain room, or in some other place or with a certain person there may be instruments that were used during the crime, objects and valuables resulting from the crime as well as other objects and documents which might present interest for the criminal case. (2) A search may also be performed for the purpose to find a wanted person, or human or animal corpses. (3) A search is carried out based on the motivated ordinance issued by the criminal prosecution body and exclusively with the authorisation of the instruction judge. (4) In cases of the flagrante depcto, a search may be done based on the motivated ordinance without having an autorisation of the instruction judge, and to submit to the latter immediately, but not later than 24 hours from the moment of termination of the search the materials obtained in the result of the search, with the motives of search indicated. The instruction judge will verify the legality of the procedural action. (5) In case of establishment of the fact that the search was legally conducted,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	the instruction judge will confirm its result by a resolution. Contrarily, the search will be considered illegal by a motivated court order. **Article 126. Grounds for Seizing Objects or Documents** (1) The criminal investigative body shall have the right to seize any objects or documents important for the criminal case if the evidence obtained or the operative investigative materials refer precisely to the place and the person holding them. (2) The seizure of documents containing information that is a state, trade, banking secret and the seizure of information on telephone conversations shall be allowed only upon the authorization of the investigative judge. (3) The seizure of objects or documents in other circumstances shall be based on a reasoned ruling by the criminal investigative body.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be	**Law on preventing and combating cybercrime, nr. 20-XVI, 03.02.2009** **Article 6. Obligations of owners of systems computer** 7. The obligations of service providers (1) service providers are obliged: f) ensure monitoring, supervision and retention of traffic data for a period of at least 180 calendar days, for the identification of service providers, service users and the channel through which the communication was transmitted to the instrumentality; **Article 7. Obligations of service providers** (1) Service providers are obliged: a) to keep records of service users; b) to notify the competent authorities about the web traffic data, including the data about illegal access to computer system information, about the attempts to introduce illegal programs, about the violation by competent persons of the rules of collection, processing, storage, transmission and distribution of information or of rules of computer system protection provided according to the information importance or to its degree of protection, if they have contributed to acquisition, distortion or destruction of information or if they have caused other serious consequences, perturbation of computer systems functioning and other

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	computer crimes; c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of web traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation; d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user; e) to undertake security measures by means of using some procedures, devices or specialized computer programs, with the help of which to restrict or forbid the unauthorized users to access a computer system; f) to ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted g) to ensure the interpretation of computer data from network protocols packages, preserving such data for a period of at least 90 calendar days. (2) If the web traffic data are possessed by several service providers, then the requested service provider is obliged to submit to the competent authority the necessary information for the identification of the other service providers. **Law on Special Investigative Activity** **Article 18. Special investigative measures** (1) In order to fulfill the tasks under this law may be performed the following special investigative measures: 1) with the authorization of the investigating judge, at the request of the prosecutor: a) research of the home and / or the installation of appliances in it, that ensure the audio and video supervision and recording, namely those for photo and filming; b) supervise the home by using technical recording means; c) the interception and recording of communications and images; d) retention, research, deliver, searches or seizure of postal items; e) monitoring the telegraph and electronic communication connections;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	f) monitoring and control of the financial transactions and access to financial information; g) documentation using technical methods and means, as well as locating or perusing by global positioning system (GPS) or by other technical means; h) collection of the information by the electronic communication service providers; 2) with the authorization of the prosecutor: a) to identify the subscriber, the owner or user of an electronic communication system or of an access point to an IT system; b) visual tracking; c) control of the money transmission or other tangible extorted assets; d) undercover investigation; e) cross-border supervision; f) controlled delivery; g) collecting samples for comparative research; h) research the objects and documents; i) acquisition of control; 3) with the authorization of the head of the specialized subdivision: a) questioning; b) collecting information about people and events; c) identify the person. (2) The list of the measures specified in par. (1) is exhaustive and may be modified only by the law. (3) The measures provided in paragraph. (1) point 1), and par. (1) point 2). c), e) and f) are performed only in a criminal process under the Criminal Procedure Code of the Republic of Moldova. Other measures prescribed by paragraph. (1) point 2) are done both in a criminal process, as well as outside it. The measures provided in the paragraph. (1) point 3) are carried out outside the criminal process. (31) The measures provided by the para. (1) point 1) letter c), g) and h), as well as those provided at the para (1) point 2) could be performed outside the criminal investigation process, within the professional integrity test, with the authorization of the judge, according to the Law no. 325 of 23 December 2013 on the evaluation of the institutional integrity. [Art.18 para.(31) introduced by the LP102 of 21.07.16, MO256-267/12.08.16 Art.547; in force 12.11.16] (4) Special investigative measures under par. (1) point 2). c) are performed

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	only by specialized subdivisions of the Ministry of Interior and National Anti-Corruption Center. (5) During the performance of special investigative measures are used IT systems, video and audio recording equipment, photo and filming cameras, other technical means, if they were authorized as required by the law. (6) The organization, methods of performing the special investigative measures, internal authorization procedures, the rules of drawing up protocols on the management, preservation and destruction of obtained objects, the measures to ensure their integrity and confidentiality and the confidentiality of special investigative activities, the rules of carrying out undercover operations, and in regard to the lead and management of the undercover activity performed undercover, the modality of registration of the special files, as well as the usage of the financial resources assigned for carrying out the special investigative measures, are established by common regulation of the authorities performing special investigative activity in agreement with the General Prosecutor's Office. **Article 24. Using the results of the special investigative measures** (1) The results of special investigative measures may serve as a reason for carrying out other special investigative measures to prevent crime and state security, for public order, as well as evidences, if they were performed within a criminal case. (2) Information about the forces (except of those providing support to authorities carrying out special investigative measures), means, sources, methods, plans and results of special investigation activity, as well as the organization and tactics of carrying out special investigative measures, which are state secret, can be declassified only in accordance with law. (3) If the investigative officer finds a reasonable suspicion of committing or preparing to commit an offense, he/she shall immediately sent all materials, by a report, to the criminal investigation body. (3) Using the results of a special investigative measure specified in art. Article 18. (1) point 2) from a special file in another special case is made only with the authorization of the prosecutor who authorized the original measure.
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	**Law on preventing and combating cybercrime, nr. 20-XVI, 03.02.2009**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 6. Obligations of owners of systems computer** 7. The obligations of service providers (1) service providers are obliged: b) to communicate to the competent authorities information about traffic data, including data on illegal access to information from the computer system, about the pitfalls of introducing illegal programs about violations by persons in charge of the rules for the collection, processing, storage, transmission, information sharing, and the rules of protection of computer system specified in accordance with the statute or its information with degree of protection If they have contributed to the appropriation, distortion or destruction of the information or have caused serious disruption to track other functioning information systems and other computer-related crime; **Code of Criminal Procedure** **Article 135. Interception of communication** (1) Interception of communication (the telephone conversations, via the radio or using other technical means) is done by the criminal prosecution body based on the authorization of the instruction judge, based on motivated ordinance of the prosecutor, in cases regarding the extremely serious and exceptionally serous crimes. (2) In case of urgency, when a delay as stipulated in the paragraph (1) could cause severe harm to the evidence collection procedure, the prosecutor may issue a motivated ordinance allowing interception and recording of communications. S/he is obpgated to inform the instruction judge about this immediately, but no later than 24 hours. The latter, in no less than 24 hours period of time is supposed to take an attitude regarding the ordinance issued by the prosecutor. When s/he confirms it s/he further authorises the interception in case of necessity. When s/he doesn't confirm it s/he requests its immediate suspension and destruction of already made records. (3) Interception of communication may be made at the request of the damaged party, the witness and members of his/her family in case of threats of violence, extortion or commission of other crimes regarding these people, based on a motivated ordinance of the prosecutor. (4) Interception of communication during criminal investigation is authorised for maximum 30 days duration. Interception may be prolonged in the same conditions based on justifiable reasons. Each prolongation however will not exceed 30 days. The total term will not exceed 6 months. In any case it may not

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	last longer then the criminal prosecution. (5) Interception of communications may be stopped before the end of the period for which it had been authorised, immediately after disappearance of grounds that justified it. (6) During the criminal prosecution the instruction judge, after the end of an authorised interception, requests opinion of the prosecutor who supervises and carries out the criminal prosecution, in reasonable terms, but not later than the termination of the criminal prosecution, announces in written form the persons whose conversations were intercepted and recorded. **Article 136. Interception and recording and their authorization** (1) Interception of communications are carried out by the criminal prosecution body. Persons whose responsibility is to technically faciptate interception and recording of communications are obliged to preserve the secret of the procedural action and confidentiality of correspondence. They are liable in case of violation of their obligation according to provisions of articles 178 and 315 of the Criminal Code. An entry regarding explaining these obligations is made in the minute of the interception. (2) A minute regarding interceptions and recording performed by the criminal prosecution body is drawn up in conformity to provisions of articles 260 and 261. The authority given by the instruction judge is additionally mentioned here along with the indication of telephone number, or numbers, the addresses of the telephone posts, radio or other technical means used to carry out the conversations. The record will also indicate the name of persons, whenever they are known, date and time of each separate conversation and number assigned to the tape used for recording. (3) Recorded communications are integrally transcribed and annexed to the minutes along with the authorization from the criminal prosecution body, after its verification and signing by the prosecutor carrying out or supervising the criminal prosecution. Correspondence in other languages than the one in which the criminal prosecution is carried out is translated with the assistance of an interpreter. The tape containing the original recorded communication is also annexed to the minutes after having been sealed and the stamp of criminal investigation body has been applied. (4) The tape with the recorded communication, its written version on paper and the minutes of the interception and recording of communications are handed over to the prosecutor within 24 hours period of time. The prosecutor assesses which one of the collected information is important for the respective case and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	draws a minutes in this respect. (5) Original copies of the tapes along with the integral written version on paper and copies of minutes are handed over to the instruction judge who authorized interception of the communication for further storage in special place, in the sealed envelope. (6) The court makes a decision or passes a sentence regarding destruction of records which are not important for the criminal case. All the other records will be kept up to the moment when the file is submitted to the archive. **Article 138. Verification of interception recording** Evidence collected under provisions in articles 135 and 137 may be verified through technical expertise ordered by the court at the request of parties or ex officio. 7. The obligations of service providers (1) service providers are obliged: a) to keep track of users of services; b) to communicate to the competent authorities information about traffic data, including data on illegal access to information from the computer system, about the pitfalls of introducing illegal programs about violations by persons in charge of the rules for the collection, processing, storage, transmission, information sharing, and the rules of protection of computer system specified in accordance with the statute or its information with degree of protection If they have contributed to the appropriation, distortion or destruction of the information or have caused serious disruption to track other functioning information systems and other computer-related crime;
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:	***THE CRIMINAL CODE*** ***OF THE REPUBLIC OF MOLDOVA*** **Article 11. Application of Criminal Law in Space** (1) All persons who committed crimes in the territory of the Republic of Moldova shall be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	held criminally liable under this Code. (2) Citizens of the Republic of Moldova and stateless persons with permanent domiciles in the territory of the Republic of Moldova who commit crimes outside the territory of the country shall be liable for criminal responsibility hereunder. (3) If not convicted in a foreign state, foreign citizens and stateless persons without permanent 16 domiciles in the territory of the Republic of Moldova who commit crimes outside the territory of the Republic of Moldova shall be criminally liable under this Code and shall be subject to criminal liability in the territory of the Republic of Moldova provided that the crimes committed are adverse to the interests of the Republic of Moldova or to the peace and security of humanity, or constitute war crimes including crimes set forth in the international treaties to which the Republic of Moldova is a party. (4) Criminal law shall not apply to crimes committed by the diplomatic representatives of foreign states or by other persons who under international treaties are not subject to the criminal jurisdiction of the Republic of Moldova. (5) Crimes committed in the territorial waters or the air space of the Republic of Moldova are considered to be committed in
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.	**Articles 541 – 550 of Criminal Procedure Code** **Article 241. Research to Serve a Summons** Should the person summoned change his/her address, the agent shall post the summons on the door of the dwelling indicated in the summons and shall undertake research to find out the new address. Any data collected shall be mentioned in the transcript.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and 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	**Article 242. Confirmation of the Receipt and Transcript of Serving a Summons** (1) The confirmation of receipt of a summons shall include the number of the criminal case, the name of the criminal investigative body or the court issuing the summons, the last name, first name and procedural capacity of the person summoned, and the date the person summoned is supposed to appear before the respective body. The confirmation of receipt shall also refer to the date the summons was served and shall include the last name, first name, capacity and signature of the person serving the summons, certification by him/her of the identity and the signature of the person served the summons and the specification of this person's capacity. (2) Whenever transcript of serving or posting a summons is prepared, it shall correspondingly cover the data indicated in para. (1) **Article 243. Notification about Other Procedural Acts** Notification about other procedural acts shall be performed in line with the provisions of this Chapter. **Article 244. Requests and Motions** (1) Requests in a criminal proceeding are written or oral applications addressed by the parties in the proceeding or other interested persons to the criminal investigative body or to the court in connection with the unfolding of the proceeding and the establishment of circumstances important for the case and those ensuring the legal rights and interests of the person. (2) Motions are the acts of criminal investigative bodies, public organizations or a team of employees aimed at specific procedural actions performed in line with this Code. The motions of a criminal investigative body shall be addressed to the investigative judge or, as the case 143 may be, to the court. The motions of public organizations and teams of employees shall be addressed to the criminal investigative body or to the court. **Article 245. Filing Requests and Motions** (1) Requests and motions may be filed at any stage of a criminal proceeding. The person filing the request or motion shall refer to the circumstance in which

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
updated a register of authorities so designated by the Parties. Each Party shall ensure	he/she is requesting the procedural action to be performed or a judgment to be issued. Written requests and motions shall be attached to the criminal case file while oral ones shall be included in the transcript of the procedural action or the transcript of the court hearing. (2) Rejecting a request or motion shall not deprive the person, public organization or team of employees of the right to repeatedly file one at a different stage in the criminal proceeding. **Article 246. Timeframes for the Examination of Requests and Motions** (1) Requests and motions filed by public organizations and teams of employees shall be examined and settled immediately after they have been filed. Should the body to which the request or motion is addressed be unable to settle it immediately, it shall settle it not later than within three days from the date of its receipt. (2) The motions of a criminal investigative body shall be examined within the timeframes set by this Code. **Article 247. Settling Requests and Motions** (1) The request or, as the case may be, the motion of a public organization or of a team of employees shall be accepted if it contributes to a comprehensive, complete and objective investigation of case circumstances and to ensuring the observance of the legal rights and interests of the parties in the proceeding and other persons participating in the proceeding. (2) If the request or, as the case may be, the motion of a public organization or a team of employees is integrally or partially rejected, the criminal investigative body shall adopt an order and the court a ruling that shall be brought to the notice of the applicant. The judgment of the criminal investigative body or the court on rejecting a request or motion may be appealed in the cases and in the manner set out in this Code. (3) The motions of a criminal investigative body shall be examined in the manner duly set out in this Code. **Article 248. Amending Procedural Acts** (1) Any amendment (completion, correction, deletion) of the contents of a procedural act shall be valid if it is confirmed in writing in the text or at the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	bottom of the act by the signatories. (2) Unconfirmed amendments shall be valid provided they do not change the meaning of the phrase. (3) Empty spaces in a declaration shall be struck through so that it is impossible to add any text in the space. **Article 249. Correcting Material Errors** (1) Obvious material errors in the contents of a procedural act shall be corrected by a criminal investigative body, the investigative judge or the court that issued the act at the request of an interested person or ex officio. (2) Upon the correction of substantive errors, the parties may be summoned to provide explanations. (3) The criminal investigative body shall prepare transcript of the correction and the investigative judge or the court shall prepare a ruling. A note to that effect shall be made at the bottom of the corrected act. **Article 250. Eliminating an Obvious Omission** The provisions art. 249 shall also apply when, as a result of an obvious omission, the criminal investigative body, the investigative judge or the court does not express an opinion on the amounts claimed by the witnesses, experts, interpreters, translators or defense counsels on the return of objects or material evidence or the revocation of security measures or of other measures.
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use	**Articles 531 – 540 of Criminal Procedure Code** **Article 531. Legal regulation of international legal assistance** (1) The relationships with foreign countries or international courts regarding the legal assistance in criminal matters shall be regulated by the present Chapter. The provisions of international treaties to which the Republic of Moldova is a party to as well other international commitments of the Republic of Moldova shall have priority in relation with the provisions of this Chapter. (2) If the Republic of Moldova is a party to several international acts of legal assistance and the foreign state from which legal assistance is solicited or which solicits it, and if there are divergences or incompatibilities between the provisions of these acts, than the provisions of the treaty which ensures a better

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	protection of the human rights and freedoms shall be applied. (3) The admissibility of granting international legal assistance shall be decided by the competent court. The Ministry of Justice may decide the non-execution of a judgement regarding the admission of granting international legal assistance when the fundamental national interests are at stake. **Article 532. Manner of transmission of the legal assistance' addressing** Addressing concerning international legal assistance in the criminal maters shall be made through the mediation of the Ministry of Justice, of the General Prosecutor's Office directly and/or through the mediation of the Ministry of External Affairs of the Republic of Moldova, except for the cases when on the basis of mutuality another manner of addressing is provided. **Article 533. Extent of legal assistance** (1) international legal assistance may be solicited or granted at the execution of certain procedural activities provided by the criminal procedure law of the Republic of Moldova and of the respective foreign state, namely in: 1) transmission of acts to natural persons or legal entities which are abroad the borders of the country; 2) hearing of persons as witnesses or experts; 3) execution of the investigation, search, seizure of objects and documents and their transmission abroad, conduction of expert examination; 4) summoning of the persons from abroad to present voluntary in front of the criminal prosecution or of the court for hearing or confrontation, as well as forced bringing of the persons in detention at that moment; 5) conduction of criminal prosecution upon the denunciation made by a foreign state; 6) search and extradition of the persons who had committed crimes or for the execution of the imprisonment sentence; 7) recognition and execution of the foreign sentences; 8) transfer of the convicted persons;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	9) other actions which do not contravene to the present Code. (2) Taking of the preventive measures shall not be an object of the international legal assistance. **Article 534. Refusal of international legal assistance** (1) International legal assistance may be refused, if: 1) the request refers to crimes considered in the Republic of Moldova as being political or connected crimes to such political crimes. The refusal shall be inadmissible if the person is suspected, accused or convicted for the commission of perpetration provided in art.5-8 of the Rome Status of the International Court of Criminal Justice; 2) the request refers to a perpetration which constitutes exclusively a violation of the military discipline 3) the criminal prosecution body or court which is solicited to grant legal assistance considers that its execution may violate the sovereignty, security or public order of the country; 4) the are founded grounds to believe that the suspect is prosecuted or punished for reasons of race, religion, nationality, membership of a certain group or for sharing certain political beliefs, or if his situation is even more aggravated due to the listed reasons; 5) the respective perpetration is punished with death according to the legislation of the soliciting state and the soliciting state offers no guarantee of non-application of the capital punishment 6) according to the Criminal code of the Republic of Moldova the perpetration invoked in the request does not represent a criminal offence; 7) according to the domestic legislation the person can not be held criminally liable. (2) Refusal of international legal assistance shall be motivated if this obligation flows from the treaty the Republic of Moldova is a party to. **Article 535. Expenses related to granting legal assistance** Expenses related to granting legal assistance shall be covered by the soliciting party from the territory of its country if another way of covering the expenses in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the conditions of mutuality or in an international treaty is not established. **Article 536. Addressing with a rogatory commission** (1) If the criminal prosecution body or the court considers necessary taking a procedural action on the territory of a foreign state it shall address with a rogatory commission to the respective criminal prosecution body or court from the respective state or to an international criminal court, according to the provisions of the international treaty to which the Republic of Moldova is a party to or under mutuality conditions. (2) Mutuality conditions shall be confirmed by a letter through which the Minister of Justice or the General Prosecutor of the Republic of Moldova undertakes in the name of the Republic of Moldova to grant legal assistance to the foreign state or to the international criminal court in taking some procedural actions with securing of procedural rights provided by the domestic law concerning whom the assistance is granted.. (3) The rogatory commission in the Republic of Moldova shall be submitted by the criminal prosecution body to the Prosecutor General, and by the court - to the Minister of Justice in order to be transmitted for execution to the respective foreign state. (4) The rogatory commission request and the documents attached to it shall be translated in the official language of that state or of that international criminal court to which it addresses. **Article 537. Content and form of request on rogatory commission** (1) Request on the rogatory commission shall be made in written and shall include the following data: 1) name of the body to which addresses the request; 2) name and address, if known, of the institution to which the request is sent; 3) international treaty or agreement of mutuality based on which assistance is requested; 4) indication of the criminal case in which it is solicited granting of legal assistance, information on the circumstances of the facts in which the actions had been committed and their legal qualification, the text of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	respective article from the Criminal Code of the Republic of Moldova and data on the caused damage by the respective crime 5) data on the persons regarding whom the rogatory commission is requested, including information on their procedural capacity, their date and place of birth, nationality, domicile, occupation, for the legal entities - name and premises, as well as the names and addresses of the representatives of this person when it is the case; 6) object of the request and necessary data for its fulfilment with the statement of the circumstances to be found, the list of the documents, corpus delicti and of other proofs requested, the circumstances in relation to which the evidence has to be administrated, as well as the questions to the asked the persons to be heard. (2) Request on the rogatory commission and the documents attached to it shall be signed and authenticated with the official stamp of the competent soliciting institution. **Article 538. Validity of the procedural act** The procedural act drawn up in a foreign country according to the legal provisions of that country shall be valid before the criminal prosecution bodies and courts from the Republic of Moldova, when its execution is performed according to the procedure provided by the present Code. **Article 539. Summoning of the witness or expert who is outside the borders of the Republic of Moldova** (1) The witness or the expert may be summoned by the body conducting the criminal prosecution for the execution of certain procedural actions on the territory of the Republic of Moldova in case of their acceptance to show up in front of the soliciting body. (2) Summoning of the witness or expert shall be made under the conditions provided by art.536, par.(3) and (4). (3) Procedural actions with the participation of the persons summoned according to the provisions of this article shall be taken in compliance with the present Code. (4) The witness or the expert, regardless nationality, who has presented himself

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	after being summoned as provided by this article in front of the soliciting body, may not prosecuted, detained or subjected to any individual freedom limitation on the territory of the Republic of Moldova for perpetrations or convictions prior to crossing the Republic of Moldova's borders. (5) The immunity provided by par.(4) ends if the witness or expert has not left the territory of the Republic of Moldova within 15 days from the date when he was called and communicated by the respective body that his presence is not necessary any more, or when he came back later on in the Republic of Moldova. This term does not include the period of time when the witness or expert was not able to leave the territory of the Republic of Moldova because on reasons independent from his will. (6) The summoning of the detained person in a foreign state shall be made according to the provisions of this article with the condition that the person temporary transferred on the territory of the Republic of Moldova by the respective body from the foreign state in order to take the actions indicated in the request on his transfer shall be returned in the time indicated in the request. The transfer conditions or its refusal shall be regulated by the international treaties to which the Republic of Moldova and the solicited state are parties to or on the grounds of written obligations in mutuality conditions. **Article 540. Execution of the rogatory commission requested by foreign bodies in the Republic of Moldova** (1) Criminal prosecution body or the court shall perform rogatory commissions requested by the respective foreign bodies on the basis of the international treaties to which the Republic of Moldova and the foreign soliciting state are parties to or in mutuality conditions confirmed according to the provisions of art.536, par.(2). (2) The request for the performance of the rogatory commission shall be sent by the Prosecutor General to the criminal prosecution body or, upon the case, by the Minister of Justice to the court at the place where the solicited procedural action will be taken. (3) The request on hearing the witness or the expert shall be executed in all the cases by the instruction judge.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) At the execution of the rogatory commission the provisions of the present Code shall be applicable, but, upon the request of the soliciting party a special procedure provided by the legislation of the foreign state may be applied, in compliance with the respective international treaty or with the observance of the mutuality conditions if this complies with the domestic legislation and with the international obligations undertaken by the Republic of Moldova. (5) Representatives of the foreign state or of the international instance may assist at the execution of the rogatory commission, if this is provided by the respective international treaty or by an obligation provided in written by the mutuality conditions. In such a case, upon the request of the soliciting party, the body which has to execute the rogatory commission shall inform the soliciting party on the time, place and term of the rogatory commission's execution in order for the interested party to be able to assist. (6) If the address of the person, with respect to whom the rogatory commission is solicited, is indicated mistakenly, the body charged with execution shall take the respective measures for finding the address. If the finding of the address is not possible, the soliciting party shall be announced. (7) If the rogatory commission may not be performed, the received documents shall be returned to the soliciting party through the mediation of the institution from which the documents have been received, with the indication of the reasons which have impeded the execution. The request on the rogatory commission and the attached documents shall be returned in the refusal cases as well, on the grounds provided by the article 534.
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.	**Chapter III INTERNATIONAL COOPERATION** **Article 8. International cooperation of the authorities the competent** (1) the competent authorities shall cooperate in accordance with the law, observing the obligations provided for in international treaties to which Moldova is a party, with institutions that have similar powers in other States and with international organizations specializing in this field. (2) provides for Collaboration: international legal assistance in criminal matters;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	extradition; identification; blocking, seizing and confiscation of the proceeds and instruments of crime; common enquiries; the exchange of information; specialized training of personnel; similar activities. **Article 9. Operative investigation activity and the prosecution held jointly** (1) at the request of the competent national authorities of other States, or within the territory of the Republic of Moldova may be held under the law, operative investigation activity in the prosecution of the common purpose of prevention and the fight against cybercrime. (2) joint investigations and will take place on the basis of bilateral or multilateral agreements concluded by the competent authorities. (3) the representatives of the competent authorities of the Republic of Moldova can participate in joint investigations carried out in the territory of other States, in accordance with their legislation. Article 10. Requests the competent authorities Foreign (1) within the framework of international cooperation, the foreign competent authority may request the competent authority in the Republic of Moldova the immediate preservation of computer data or computer data on traffic, existing in a computer system in the territory of the Republic of Moldova concerning the foreign competent authority will formulate a reasoned request, international legal assistance in criminal matters. (2) the request for the immediate conservation measures referred to in paragraph 1.(l) include: name of requesting authority); b brief presentation of the facts) that are the subject of criminal prosecution and legal argumentation; c) computer data that is requested to be preserved; d) any available information necessary for identification of the holder of the data processing, the location information system; e) usefulness of computer data, the need for their conservation; f) foreign competent authority's intention to make a request for international legal assistance in criminal matters. (3) the period of storage of data recorded at para.(l) may not be less than 60 calendar days and shall be valid until the competent national authorities shall decide on the request for international legal assistance in criminal matters.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) the transmission of computer data will be performed only after acceptance of the application of international legal assistance in criminal matters.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall,	If there is no mutual assistance treaty or arrangement the General Prosecutor's Office sends request basing on the principle of goodwill and reciprocity. The Central Authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution: *pre-trial investigation* – **the General Prosecutor's Office,** *trial* **– the Ministry of Justice**. **Article 534. Rejecting International Legal Assistance** (1) International legal assistance may be rejected if: 1) the request refers to crimes considered in the Republic of Moldova political crimes or crimes related to such crimes. The rejection shall not be admitted if a person is suspected, accused or was convicted for the commission of certain acts provided in arts. 5–8 of the Rome Statute of the International Criminal Court; 2) the request refers toan act exclusively constituting a violation of military discipline; 3) the criminal investigative body or the court to which the request for legal assistance was addressed considers that its execution is of a nature to affect the sovereignty, security or public order of the state; 4) there are grounds for believing that the suspect is being criminally pursued or punished due to his/her race, religion, citizenship, association with a certain group or certain political beliefs, or if his/her situation will be exacerbated for the aforementioned reasons; 5) it is proven that the person will not have access to a fair trial in the requesting state; 6) the respective act is punished by death as per the legislation of the requesting state and the requesting state provides no guarantee in view of not applying or not executing capital punishment; 7) in line with the Criminal Code of the Republic of Moldova the act or acts invoked in the request do not constitute a crime; 8) in line with national legislation the person may not be subject to criminal liability. (2) Any rejection of international legal assistance shall be reasoned.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of	**The Law on mutual legal assistance in criminal matters no. 371-XVI din 01.12.2006**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**Art 6. Confidentiality** (1) The Republic of Moldova shall ensure, within the limits of law, at the request of the Requesting State, confidentiality of the requests for legal assistance and documents enclosed. If the condition of confidentiality cannot be assured, Moldova will notify the foreign state that will decide. (2) The provisions of paragraph (1) shall be applied when the Republic of Moldova is the Requesting State.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of	**Please refer to Convention Article 16 above**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall	**Please refer to Convention Article 17 above**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Please refer to Convention Article 18 above**
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time	**Please refer to Convention Article 20 above**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**Please refer to Convention Article 21 above**
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available,	**Center for Combating Cyber Crime** **IT and fighting cyber crime section** In Moldova there are two 24/7 contact points 1. The first contact point 24/7 is located in the The Center for Combating Cyber Crime of National Inspectorate for Investigations GPI of 2. The second 24/7 contact point is located in the general prosecutor's office, in the specialized division - IT and cyber crime investigations section.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents