Lithuania

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 01 May 2020

[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	No additional provisions except the definitions listed in Convention. After ratification of the Convention it is the Law and part of national legislation. Below listed articles are parts of the Criminal Code and Code of Criminal Procedure
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	1. Any person, who misappropriates the legally protected computer information about a legal or natural person, shall be punished by a fine, or imprisonment for a term of up to 3 years. 2. Any person, who publicly spreads, discloses or disseminates or in other way uses information obtained by committing the acts specified in Paragraph 1 of this Article, shall be punished by a fine, or arrest, or imprisonment for a term of up to 4 years. 3. Any legal person shall also be held liable for the acts provided for in this Article. **Article 198(1). Unlawful Connection to an Information System** 1. A person who unlawfully connects to an information system by damaging the protection means of the information system shall be punished by community service or by a fine or by arrest or by imprisonment for a term of up to one year. 2. A person who unlawfully connects to an information system of strategic importance for national security or of major importance for state government, the economy or the financial system shall be punished by a fine or by arrest or by imprisonment for a term of up to three years. 3. A legal entity shall also be held liable.
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	3. A legal entity shall also be held liable for the acts provided for in this Article.
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 196. Destruction or Change of Computer Information.** 1. Any person, who destroys, damages, removes or changes computer information, or who restricts access to this kind of information by means of devices or computer programs, thus causing serious damage, shall be punished by community service, or a fine, or imprisonment for a term of up to 3 years. 2. Any legal person shall also be held liable for the acts specified in this Article. Article 196. Unlawful Influence on Electronic Data 1. A person who unlawfully destroys, damages, removes or modifies electronic data or a technical equipment, software or otherwise restricts the use of such data thereby incurring major damage shall be punished by community service or by a fine or by imprisonment for a term of up to four years. 2. A person who commits the act provided for in paragraph 1 of this Article in respect of the electronic data of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system shall be punished by a fine or by arrest or by imprisonment for a term of up to six years. 3. A person who commits the act provided for in this Article thereby incurring minor damage shall be considered to have committed a misdemeanour and shall be punished by community service or by a fine or by restriction of liberty or by arrest. 4. A legal entity shall also be held liable for the acts provided for in this Article.
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 197. Unlawful Influence on an Information System** 1. A person who unlawfully disturbs or terminates the operation of an information system thereby incurring major damage shall be punished by a fine or by arrest or by imprisonment for a term of up to four years. 2. A person who commits the act provided for in paragraph 1 of this Article in respect of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system shall be punished by a fine or by arrest or by imprisonment for a term of up to six years. 3. A person who commits the act provided for in this Article thereby incurring

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	minor damage shall be considered to have committed a misdemeanour and shall be punished by community service or by a fine or by restriction of liberty or by arrest. 4. A legal entity shall also be held liable for the acts provided for in this Article..
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	**Article 198(2). Unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data** 1. A person who unlawfully produces, transports, sells or otherwise distributes the installations or software, also passwords, login codes or other similar data directly intended for the commission of criminal acts or acquires or stores them for the same purpose shall be punished by community service or by a fine or by arrest or by imprisonment for a term of up to three years. 2. A legal entity shall also be held liable for the acts provided for in this Article. .
Title 2 – Computer-related offences	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Article 214. Production or disposition of the other means of payment** **Article 215. Use of the illegal mean of payment or its data**
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 182. Fraud.** 1. Any person who, for his personal or other's advantage, by fraud obtains property or property right belonging to another person, evades or eliminates pecuniary obligation, shall be punished by community service or a fine, or restriction of liberty, or detention, or imprisonment for a term of up to 3 years. 2. Any person who, for his personal or other's advantage, by fraud obtains property or property right of high value belonging to another person, evades or eliminates pecuniary obligation of the same value, shall be punished by imprisonment for a term of up to 8 years. 3. Any person who, for his personal or other's advantage, by fraud obtains property or property right of low value belonging to another person, evades or eliminates a pecuniary obligation of the same value, commits a misdemeanour, and shall be punished by community service, or a fine, or restriction of liberty, or detention. 4. The person shall be held liable for acts specified in Paragraphs 1 and 3 of this Article only in case a claim of the victim or a statement by his legal representative or a request by the prosecutor exists. 5. Any legal persons shall also be held liable for acts specified in Paragraphs 1 and 2 of this Article. **Article 196. Destruction or Change of Computer Information.** 1. Any person, who destroys, damages, removes or changes computer information, or who restricts access to this kind of information by means of devices or computer programs, thus causing serious damage, shall be punished by community service, or a fine, or imprisonment for a term of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	up to 3 years. 2. Any legal person shall also be held liable for the acts specified in this Article. **Article 197. Destruction or Replacement of Software, Disruption of the Operation of Computer Network, Data bank or Information System** 1. Any person, who illegally destroys, damages, removes or replaces the software in a computer, or disrupts or changes the operation of a computer network, database or information thus causing serious damage, shall be punished by a fine, or imprisonment for a term of up to 3 years. 2. Any legal person shall also be held liable for the acts specified in this Article.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 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-	**Article 162. The Use of a Child for Pornography** 1. Any person who exploited a child to produce a pornography, shall be punished by a fine, or imprisonment for a term of up to 4 years. 2. Any legal person shall also be held liable for the acts specified in this Article. **Article 309. Possession of Pornographic Material** (..) 2. Any person who produced, acquired, possessed, publicly displays or advertises objects of a pornographic nature which represent a child or simulate a child, shall be punished by a fine or imprisonment for a term of up to 2 years. (..) 4. Any legal persons shall also be held liable for acts specified in Paragraphs 1 and 2 of this Article.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Article 192. Unlawful Reproduction of Works of Literature, Science, Art or Other Works, Distributing, Transporting or Storing Illegal Copies Thereof.** 1. Any person, who unlawfully makes reproductions of works of literature, science, art or other works, or parts thereof, or who for the commercial purposes imports, exports, distributes, transports or stores illegal copies thereof, where the total value of copies in retail prices of legal copies exceeds the sum of 100 MSLs (minimum standards of living), shall be punished by community service or a fine, or restriction of liberty, or detention, or imprisonment for a term of up to 2 years. **Article 193. Destruction of the Information of Copyright and Related Rights** **Article 194. Unlawful Elimination of the Technical Protection of Copyright and Related Rights**
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting	**Article 25. Conspiracy and Forms of Conspiracy**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to 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.	1. Conspiracy is the intentional involvement in the commission of a criminal act by two or more conspiring legally capable persons who have attained the age specified in Article 13 of this Code. 2. The conspirators in the criminal act shall include a perpetrator, an organiser, an abettor and an accessory. 3. The perpetrator is a person who actually commits the criminal act either by himself or by causing an incapacitated person or a person who has not yet attained the age specified in Article 13 of this Code or any other person who is not of a culpable mental state to commit the act. If the act is carried out by several persons acting together, each person is considered a perpetrator (co-perpetrator). 4. The organiser is a person who forms a group of conspirators, an organised group or a criminal association, heads the group or coordinates the activities of its members, or makes preparations for a criminal act and oversees its commission. 5. The abettor is a person who incites another person to commit a specific criminal act. 6. The accessory is a person who aids, counsels or commands another in the commission of a criminal act, or who provides advices, instructions, means or removes obstacles, or who protects or shields other accomplices, or who promises in advance to harbour the offender, or to hide the instruments or means of crime, the traces of the act or the goods acquired by criminal means, or who promises in advance to sell goods produced or acquired in the course of the criminal act.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a	**Article 22. Criminal Liability of Enterprises** 1. An enterprise may be found guilty of the commission of a criminal act if such liability is foreseen in the Special Part of this Code. 2. An enterprise may be liable for the commission of a criminal act committed by the natural person only if a criminal act in the favour or interests of the enterprise committed by a natural person, who acted individually or on behalf of the enterprise liability, or if a natural person being in a key position had the right: 1) to represent an enterprise or; 2) to decree on behalf of the enterprise or; 3) to administer the activity of the enterprise. 3. An enterprise may be liable for the commission of a criminal act also if committed by employee or authorized member because of insufficient

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	supervision of a person mentioned in part 2 of this Article
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.	Indicated with the Articles
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	Code of Criminal Procedure

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *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.	In general, Code of Criminal Procedure does not foresee exceptional and/or additional Conditions and Safeguards related to Cybercrime. In such cases the investigation is conducted using the appropriate Articles which correspond to certain Procedure and situation (Search, seizure, etc.)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	The **Law on the Electronic Communications** of the Republic of Lithuania, No. IX-2135, 15 April 2004 (Official Gazette, No. 69-2382, 2004) (hereinafter referred to as "the **LEC**"). Article 65 Paragraph 2 of the **LEC** provides that in order to ensure accessibility of data for the purposes of investigation, disclosure and persecution of *serious* and *grave crimes* specified in the Criminal Code of the Republic of Lithuania, providers of a public communications network and/or public electronic communications services must preserve and submit free of charge to the competent institutions, in accordance with the procedure established by the law, generated or processed data indicated in the Annex 1 "Categories of Data to be Stored" of the LEC (see below): ***„Categories Of Data To Be Stored*** ***1. Data necessary to trace and identify the source of a communication:*** *1.1. Data concerning fixed network telephony and mobile telephony:* *1.1.1. the calling telephone number;* *1.1.2. name, surname and address of the subscriber or registered user of electronic communications services;* *1.2. Data concerning Internet access, Internet e-mail and Internet telephony:* *1.2.1. the user ID(s) allocated;* *1.2.2. the user ID and telephone number allocated to any communication entering the public telephone network;* *1.2.3. the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.* ***2. Data necessary to identify the destination of a communication:*** *2.1. Data concerning fixed network telephony and mobile telephony:* *2.1.1. the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	number or numbers to which the call is routed; *2.1.2. the name(s) and address(es) of the subscriber(s) or registered user(s);* *2.2. Data concerning Internet e-mail and Internet telephony:* *2.2.1. the user ID or telephone number of the intended recipient(s) of an Internet telephony call;* *2.2.2. the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication.* ***3. Data necessary to identify the date, time and duration of communication:*** *3.1. Data concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;* *3.2. Data concerning Internet access, Internet e-mail and Internet telephony:* *3.2.1. the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;* *3.2.2. the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone.* ***4. Data necessary to identify the type of communication:*** *4.1. Data concerning fixed network telephony and mobile telephony: the telephone service used;* *4.2. Data concerning Internet e-mail and Internet telephony: the Internet service used.* ***5. Data necessary to identify users' communication equipment or what purports to be their equipment:*** *5.1. Data concerning fixed network telephony, the calling and called telephone numbers;* *5.2. Data concerning mobile telephony:* *5.2.1. the calling and called telephone numbers;* *5.2.2. the International Mobile Subscriber Identity (IMSI) of the calling party;* *5.2.3. the International Mobile Equipment Identity (IMEI) of the calling party;* *5.2.4. the IMSI of the called party;*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	5.2.5. the IMEI of the called party; *5.2.6. in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;* *5.3. concerning Internet access, Internet e-mail and Internet telephony:* *5.3.1. the calling telephone number for dial-up access;* *5.3.2. the digital subscriber line (DSL) or other end point of the originator of the communication.* *6. data necessary to identify the location of mobile communication equipment:* *6.1. the location label (Cell ID) at the start of the communication;* *6.2. data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained."* **Article 178. Actions of the Prosecutor and Pre-Trial Investigation Institutions**
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	The **Law on Operational Activities** of the Republic of Lithuania, No IX-965, 20 June 2002 (Official Gazette No. 65-2633, 2002) (as last amended on 27 March 2012, No. XI-1941, Official Gazette No. 42-2043, entered into force since 7 April, 2012) (hereinafter referred to as "the **LOA**"). The LOA regulates the legal basis for operational activities, principles and tasks of operational activities, the rights and duties of entities of operational activities, the carrying out of operational actions and operational investigation, participation of persons in operational activities, the use and disclosure of operational intelligence as well as the financing, control, and scrutiny of these activities. Article 3 of the **LOA** provides legal definitions related to operational activities:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	*"1. **Operational activities** shall mean the overt and covert intelligence activities carried out by entities of operational activities in accordance with the procedure laid down by this Law.* *2. **Targets of operational activities** shall mean the criminal acts being planned, being or having been committed, the persons planning, committing or having committed the criminal acts, active actions of these persons in neutralising operational activities or infiltrating members of criminal structures in law enforcement, national defence or other state government and administration institutions, activities of foreign special services as well as other persons and events related to state security.* *3. **Entities of operational activities** shall mean the divisions of the systems of national defence, the Interior and the customs, the State Security Department and the Special Investigation Service which have been granted special state powers and charged with the carrying out of operational activities and whose officers have been granted powers to carry them out. A list of these divisions shall be compiled and the scope of operational activities thereof shall be determined by the Government. The main institutions of entities of operational activities shall be the Second Investigation Department under the Ministry of National Defence, the Financial Crime Investigation Service under the Ministry of the Interior, the Customs Department under the Ministry of Finance, the Police Department under the Ministry of the Interior, the Special Investigation Service, the VIP Protection Department under the Ministry of the Interior, the State Security Department, and the State Border Guard Service under the Ministry of the Interior.* */.../* *8. **Use of technical means in operational activities** shall mean the installation, operation or dismantling of technical means and other lawful actions related thereto. Technical means may be used in operational activities in accordance*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	with the general and special procedure. *9. **Use of technical means in accordance with the special procedure** shall mean the use of technical means in operational activities authorised by a reasoned court ruling when monitoring or recording personal conversations, other communications or actions, where none of the participants in the conversation, other communications or actions is aware of such monitoring and it is implemented by restricting the individual's right to inviolability of private life in accordance with the procedure laid down by law. The monitoring of the content and recording of the personal information transmitted by electronic communications networks, even if one of the persons is aware of such control, shall be subject to a reasoned court ruling, with the exception of the cases when a person requests or consents to such monitoring or recording without making use of the services and equipment of the economic entities providing the electronic communications networks and/or services.* */.../* *24. **Operational investigation** shall mean an organisational tactical form of operational activities covering operational actions, including the actions requiring a reasoned court ruling or a prosecutor's authorisation. In carrying out an operational investigation, entities of operational activities may process operational investigation files."* Article 7 Paragraph 4 of the **LOA** provides rights of entities of operational activities: *"4. Entities of operational activities shall, on the grounds for an operational investigation provided for in Article 9 of this Law and upon obtaining the authorisation specified in Articles 10, 11, 12 or 13 of this Law, have the right:* *1) to covertly monitor postal items, document items, money orders and documents thereof, obtain information on the economic, financial operations of a natural or legal person and on the use of financial instruments and/or means of payment;* *2) to use technical means and obtain information from the economic entities providing electronic communications networks and/or services in accordance*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	with the special procedure; *3) in accordance with the procedure laid down by the Government upon co-ordination with the Bank of Lithuania, to obtain information from the Bank of Lithuania; to obtain information from commercial banks, other credit and financial institutions, also from other legal persons – in accordance with the procedure laid down by the Government;* *4) to covertly enter residential and non-residential premises and vehicles and to inspect them, to temporarily seize and inspect documents, seize samples of substances, raw materials and production as well as other objects for investigation without disclosing the fact of seizure thereof;* *5) to use the mode of conduct imitating a criminal act;* *6) to carry out controlled delivery."* ***Article 9. Grounds for an Operational Investigation*** *An operational investigation shall be conducted, when:* *1) characteristics of a criminal act have not been established, but information is available about a* ***grave*** *or* ***serious crime*** *being planned, being committed or having been committed or* ***less serious*** *crimes provided for in Article 131, paragraph 2 of Article 145, paragraphs 2 and 3 of Article 146, paragraph 2 of Article 151, Article 162, paragraph 2 of Article 178, paragraph 1 of Article 180, paragraph 1 of Article 181, paragraph 2 of Article 187, paragraph 2 of Article 189, paragraph 1 of Article 189[1], paragraph 2 of Article 198, paragraph 1 of Article 213, Articles 214 and 215, paragraph 1 of Article 225, paragraphs 1 and 2 of Article 226, paragraphs 1 and 2 of Article 227, paragraph 1 of Article 228, Article 228[1], Article 240, paragraph 1 of Article 253, paragraph 1 of Article 256, paragraphs 2 and 3 of Article 300, paragraph 2 of Article 301, paragraph 2 of Article 302 and paragraphs 1 and 2 of Article 307 of the Criminal Code of the Republic of Lithuania or about a person planning, committing or having committed a crime;* *2) information is available about the activities of the special services of other states;* *3) the suspect, the accused or the convicted person goes into hiding;* *4) a person is reported missing;* *5) protection of persons against criminal influence is being implemented;* *6) protection of state secrets is being implemented;*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	7) information is available about the acts positing a threat to the constitutional system of the State, independence and economic security thereof, ensuring of the defence power of the State or other interests of importance to national security." ***Article 10. Covert Monitoring of Postal Items, Document Items, Money Orders and Documents Thereof, Use of Economic, Financial Operations of a Natural or Legal Person, Financial Instruments and/or Means of Payment, Use of Technical Means in Accordance with the Special Procedure and Obtaining of Information from the Economic Entities Providing Electronic Communications Networks and/or Services, from the Bank of Lithuania, Commercial Banks, Other Credit and Financial Institutions, Also from Other Legal Persons*** *1. The covert monitoring of postal items, document items, money orders and documents thereof, the use of economic, financial operations of a natural or legal person, financial instruments and/or means of payment and the use of technical means in accordance with the special procedure shall be authorised by the chairmen of regional courts or the judges authorised by them according to reasoned applications by the Prosecutor General or prosecutors of the Prosecutor General's Office or regional prosecutor's offices who have been authorised by him and who co-ordinate and control the lawfulness of operational actions, where the applications are prepared according to the data submitted by the heads of the entities of operational activities or deputy heads authorised by them.* *2. In urgent cases, when a danger is posed to human life, health, property, public or state security, it shall be permitted to carry out the actions specified in paragraph 1 of this Article pursuant to a decision by the prosecutors listed in paragraph 1 of this Article. In such a case, a prosecutor who has taken the decision shall, within 24 hours, submit an application for the confirmation of the lawfulness or of the grounds of the actions by a reasoned ruling to a judge indicated in paragraph 1 of this Article. If the time limit expires on a day off or a holiday, the application shall be submitted on the day following the day off or the holiday. Where the judge does not confirm the grounds of the actions by a reasoned ruling, they shall be terminated, and the information*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	obtained in the course thereof shall be destroyed immediately. *3. For the purposes of conspiracy, a ruling on the carrying out of the operational actions indicated in paragraph 1 of this Article may be handed down by any regional court.* *4. An application shall indicate:* *1) the name, surname and position of the officer who has filed the application;* *2) data obtained on targets of operational activities;* *3) data (grounds) substantiating the necessity of carrying out operational actions;* *4) the economic, financial operations of a natural or legal person and/or bank account number, financial instruments and/or means of payment planned to be monitored;* *5) the postal items, document items, money orders and documents thereof planned to be monitored (when monitoring thereof is planned);* *6) duration of the application of operational actions;* *7) the result aimed at.* *5. Covert monitoring of postal items, document items, money orders and documents thereof, the use of economic, financial operations of a natural or legal person, financial instruments and/or means of payment and the use of technical means in accordance with the special procedure shall be authorised for a period not exceeding three months. This period may be extended, but not more than three successive times. The total duration of the period may not exceed 12 months.* *6. The extension of the time period provided for in paragraph 5 of this Article shall be authorised in accordance with the same procedure as the prescription of those actions. The number of extensions shall not be limited, however, each extension may not exceed a time period specified in paragraph 5 of this Article.* *7. In the event of adoption of a reasoned ruling on covert monitoring with respect to postal items, document items, money orders and documents thereof, use of economic, financial operations of a natural or legal person, financial instruments and/or means of payment, the use of technical means in accordance with the special procedure or on extension of these actions, the head of an entity of operational activities or a deputy head authorised by him shall forward one*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	copy of the ruling to the Prosecutor General or to the Deputy Prosecutor General authorised by the Prosecutor General not later than the next working day following the receipt of the ruling. *8. Where a prosecutor refuses to submit an application for authorisation of the actions specified in paragraph 1 of this Article, the head of the entity of operational activities or his authorised deputy shall have the right to refer to a superior prosecutor of those specified in paragraph 1 of this Article who has the powers to submit applications for authorisation of these actions. The refusal by the prosecutor must be substantiated in writing. The prosecutor who has taken a decision not to submit an application for authorisation of the mentioned actions must inform thereof the Prosecutor General or the Deputy Prosecutor General authorised by him. The decision of the superior prosecutor shall be final.* *9. Where the judge referred to in paragraph 1 of this Article hands down a reasoned ruling to refuse to authorise the actions specified in paragraph 1 of this Article, the prosecutor submitting the application may appeal against the ruling to the chairman of the regional court. The decision of the chairman of the regional court shall be final.* *10. Where a court hands down of a ruling, and in urgent cases, where the prosecutor specified in paragraph 1 of this Article takes a decision, an institution authorised by the Government shall notify an economic entity providing electronic communications networks and/or services of the use of technical means in its network in accordance with the special procedure indicating the application's number, the date of the handing down of the ruling and the court which has handed down the ruling or the date of the decision of the prosecutor, the prosecutor who has taken the decision as well as the duration of the application of operational actions. Responsibility for the conformity to the court ruling of the content of the notification intended for the economic entity providing electronic communications networks and/or services shall be borne in accordance with the procedure laid down by law by the officer submitting the notification. The economic entity providing electronic communications networks and/or services must take provide a technical possibility to implement monitoring of the information transmitted by means of electronic communications.* *11. The technical commands sent to the network of an economic entity providing electronic communications networks and/or services to commence or discontinue*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	wire tapping or other monitoring of the information transmitted over electronic communications networks shall be stored in such a manner that would prevent the data of the commands sent and received from being modified by the entity of operational activities which has sent the command or by the economic entity providing electronic communications networks and/or services which has received the command. An institution authorised by the Government must provide the Prosecutor General or a prosecutor authorised by him with access to the data medium which holds a record of these commands. *12. Entities of operational activities shall have the right to obtain from the economic entities providing electronic communications networks and/or services the specific information on former electronic communications events as required for an operational investigation, also information on specific operations performed with funds in an account from the Bank of Lithuania, commercial banks, other credit and financial institutions, also other legal persons upon a reasoned ruling by the chairman of a district court or a judge authorised by him, handed down in accordance with the reasoned applications of the heads of the entities of operational activities or their authorised deputies. In urgent cases, when a danger is posed to human life, health, property, public or state security, it shall be permitted to carry out the actions specified in this paragraph under decisions of heads of entities of operational activities or deputy heads authorised by them. In such a case, the heads of the entities of operational activities or the deputy heads authorised by them shall, within 24 hours, submit an application for the confirmation of the lawfulness or of the grounds of the actions by a reasoned ruling to the chairman of a district court or to a judge authorised by him. If the time limit expires on a day off or a holiday, the application shall be submitted not later than on the day following the day off or the holiday. Where the judge does not confirm the lawfulness of the mentioned actions by a reasoned ruling, the information obtained shall be destroyed immediately.* *13. In seeking to obtain the information indicated in paragraph 12 of this Article, a notice shall be submitted to the economic entities providing electronic communications networks and/or services, the Bank of Lithuania, commercial banks, other credit or financial institutions or other legal persons indicating the application number, date of adoption of the ruling and the court which has adopted the ruling. Responsibility for the conformity of this notice to the court ruling shall be borne by the officer submitting the notice in accordance with the*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	procedure laid down by law. *14. The information directly related to subscriber telephone numbers or terminal equipment of a network, to the affiliation of a telephone number or terminal equipment of a network, the account numbers of a natural or legal person or the affiliation of bank accounts and/or financial instruments and/or means of payment and the persons authorised to have it at their disposal shall not be subject to a court ruling. Specific information on the electronic communications events, economic, financial operations, the use of financial instruments and/or means of payment directly related to a person may also be collected upon this person's request or consent. This information shall be provided in accordance with the requests of officers of the entities of operational activities. Where the information is requested upon a person's request or consent, a copy of the person's request or consent shall be submitted upon prior approval by an officer submitting the request to provide information.* *15. The head of an entity of operational activities or his authorised deputy shall, in accordance with the established procedure, give a notice to the prosecutor referred to in paragraph 1 of this Article of the subscriber telephone numbers, terminal equipment of a network, accounts, financial instruments and/or means of payment, as used by a person, which were identified and became subject to covert monitoring by the entity of operational activities during the period authorised by the court. The notice of the entity of operational activities shall indicate the date and number of the court ruling, the period of validity of the authorisation, data on the person, the subscriber telephone numbers, terminal equipment of the network, financial instruments and/or means of payment subject to covert monitoring. The notice shall be sent not later than 24 hours after commencement of covert monitoring and recording of the subscriber telephone numbers, the terminal equipment of the network, the accounts, the financial instruments and/or means of payment by a decision of the head of the entity of operational activities or his authorised deputy. If the time limit expires on a day off or a holiday, the notice shall be sent not later than on the day following the day off or the holiday."* 1. The **Criminal Code** of the Republic of Lithuania, approved by the Law of the Republic of Lithuania No. VIII-1968, 26 September, 2000 (Official Gazette, No. 89-2741, No. 46, 2000) (as last amended by the Law No. XI-1861, 22

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	December, 2011, Official Gazette, No. 5-138, 2012, entered into force since 7 January, 2012) (hereinafter referred to as "the **CC**"). The CC defines which acts are crimes and misdemeanours and prohibit them; establishes penalties, penal and reformative sanctions for the acts provided for by this Code as well as compulsory medical treatment; establishes grounds for and conditions of criminal liability as well as the grounds for and conditions of releasing the persons who have committed criminal acts may be released from criminal liability or a penalty. **Article 155. The Prosecutor's Right to Examine the Information**
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	**Article 97. Exaction of the Objects and Documents relevant to Investigation**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: 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.	**Article 139. Search** 1. Upon reasonable belief that there are, in some premises or any other place, instruments of an offence, tangible objects obtained or acquired in a criminal way also objects or documents that might be relevant for the investigation. A pre-trial investigation officer or a prosecutor may carry out search with a view of discovering and seizing them. 2. A seizure may be carried out with the purpose of finding the wanted persons or bodies. 3. A search shall be carried out subject to an order of a pre-trial investigation judge. In cases of utmost urgency, a seizure may be effected under a decision of the pre-trial investigation officer or the prosecutor; however, in such cases, within three days, an approval of the pre-trial judge must be obtained about the lawfulness of such a seizure. (…) 4. A search must be carried out in the presence of the owner, tenant, manager of the flat, house or other premises where the search is being conducted, a member or their family or a close relative, and where a search is being carried out an enterprise of an office – in the presence of a representative of that enterprise or office. Where there is no possibility to ensure the presence of the above persons, a search shall be carried out in the presence of any other two persons or a representative of a municipal institution. **Article 141. Seizure** 1. If it is necessary to seize tangible objects or documents of value for the investigation, and if is known where and at whose place precisely they are, the pre-trial investigation officer or the prosecutor may effect a seizure. A seizure shall be effected under a reasoned order of the pre-trial judge. In cases of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	utmost urgency, a seizure may be effected under a decision of the pre-trial investigation officer or the prosecutor; however, in such cases, within three days, an approval of the pre-trial judge must be obtained about the lawfulness of such a seizure.(…) 2. Persons having possession of the tangible objects or documents subject to seizure must not interfere with the officers carrying out a seizure. Persons who fail to comply with this requirement may be fined under Article 163 of this Code. 3. A seizure shall be effected in the presence of the persons referred to in paragraph 4 of Article 145 of this Code. 4. If persons having possession of the tangible objects or documents subject to seizure do not agree to surrender these objects and documents voluntarily, they can be taken by force.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.	**Article 154. Monitoring and Recording of the Information Transmitted through the Telecommunications Networks**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 154. Monitoring and Recording of the Information Transmitted through the Telecommunications Networks**
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or	**Article 4. Temporal and Territorial Validity of the Code of Criminal Procedure** 1. The procedure shall be established pursuant to the Code of Criminal Procedure effective at the moment of carrying out procedural actions. 2. The procedure in the territory of the Republic of Lithuania shall be conducted pursuant to the Code of Criminal Procedure of the Republic of Lithuania, irrespective of the place where a criminal act has been committed.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	3. Where an international agreement of the Republic of Lithuania prescribes rules other than this Code, the international rules shall apply. **Article 5. Application of the Code of Criminal Procedure in Respect of Foreign Nationals and Stateless Persons** 1. The proceeding involving criminal acts committed by foreign nationals and stateless persons shall be held in the territory of the Republic of Lithuania in accordance with the Code of Criminal Procedure. 2. Where a criminal act has been committed in the territory of Lithuania by persons who, under international agreements to which the Republic of Lithuania are subject to immunity from criminal jurisdiction, the issue of their criminal liability shall be solved in accordance with treaties of the Republic of Lithuania and the Criminal Code. 3. Persons who, under international agreements of the Republic of Lithuania, are subject to immunity from criminal jurisdiction may not be arrested or detained. The procedural actions provided for in this Code may be undertaken in their respect only subject to their consent or request. The consent of said persons shall be obtained through the Ministry of Foreign Affairs of the Republic of Lithuania.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be	**Article 71. Extradition of Persons from the Republic of Lithuania or Their Transfer to the International Criminal Court** **Article 71-1. Transfer of person under the European Arrest Warrant**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.	Here and below where the boxes were left blank the International co-operation is regulated by **Articles 4, 5, 66, 67, 68, 69, 71, 72, 73, 75, 76, 77, 77-1, 94, 365** as well as by Bilateral and Multilateral Agreements **Article 4. Temporal and Territorial Validity of the Code of Criminal Procedure**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**Article 5. Application of the Code of Criminal Procedure in Respect of Foreign Nationals and Stateless Persons** **Article 66. Procedure of Communication by the Courts and the Prosecutor's Office with Counterparts in Foreign States** **Article 67. Execution of the Requests of Institutions of Foreign States for Proceedings** **Article 68. Request to Initiate Prosecution** **Article 69. Request for Extradition of a Person to a Foreign State** **Article 71. Extradition of Persons from the Republic of Lithuania or Their Transfer to the International Criminal Court** **Article 72, Arrest of Persons Whose Extradition or Transfer to the International Criminal Court is Requested** **Article 73. Procedure of Extradition of Persons from the Republic of Lithuania** **Article 75. Simplified procedure of extradition (surrender) from the Republic of Lithuania** **Article 76. The Procedure of Transfer of the Extraditable Person** **Article 77. Temporary Transfer of an Arrested or Convicted Person to Another State or the International Criminal Court for the Performance of Procedural Acts** **Article 77-1. Transit of the detained person through the territory of the Republic of Lithuania** **Article 94. Measures Taken with Regard to the tangible Objects Relevant for Investigation of a Criminal Act and the Trial in the Event of Termination of Proceedings and Rendering a Judgement**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 363. Execution of Judgements Rendered by Courts of Foreign States
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**Article 2. Duty to Detect Criminal Acts** Every time when elements of a criminal offence are discovered, the prosecutor and the institutions of pre-trial investigation must, within the limits of their competence, take all measures provided by the law to conduct an investigation, and establish that a criminal act has been committed, and the court and the judge shall ensure that the case is heard within a reasonable time by a fair and impartial court and that the guilty are prosecuted.
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;	**Article 67. Execution of the Requests of Institutions of Foreign States for Proceedings**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**Article 177. Confidentiality of the Information about a Pre-Trial Investigation** 1. Information about a pre-trial investigation shall not be made public. It may be made public only subject to a prosecutor's leave and only to such an extent as is determined as permissible. It is forbidden to public the information on underaged suspests and victims. 2. When necessary, a prosecutor or a pre-trial judge shall warn the parties to the proceedings or other persons who were witnesses to the procedural actions of the pre-trial proceedings that it is not permissible, without his authorisation, to make the information about the pre-trial investigation public. In such cases a person shall be warned and shall attest it by his signature about his liability under Article 247 of the Criminal Code of the Republic of Lithuania.
Article 29 – Expedited preservation of stored computer data	**Article 154. Monitoring and Recording of the Information Transmitted**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**through the Telecommunications Networks**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**Article 67. Execution of the Requests of Institutions of Foreign States for Proceedings**
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	**Article 67. Execution of the Requests of Institutions of Foreign States for Proceedings**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**Article 67. Execution of the Requests of Institutions of Foreign States for Proceedings**
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**Article 67. Execution of the Requests of Institutions of Foreign States for Proceedings**
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**Article 67. Execution of the Requests of Institutions of Foreign States for Proceedings**
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	International Liaison Office (Interpol) of the Lithuanian Criminal Police Bureau

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	**Declaration contained in the instrument of ratification deposited on 18 March 2004 - Or. Engl. - and confirmed by a Note verbale from the Ministry of Foreign Affairs of Lithuania, dated 26 April 2004, registered at the Secretariat General on 10 May 2004 - Or. Engl.** In accordance with Article 40 and Article 2 of the Convention, the Republic of Lithuania declares that criminal liability for the act described in Article 2 of the Convention occurs upon access to the whole or any part of a computer system without right by infringing security measures of a computer or a computer network. **Period covered: 1/7/2004 -** The preceding statement concerns Article(s) : 2 **Declaration contained in the instrument of ratification deposited on 18 March 2004 - Or. Engl. - and confirmed by a Note verbale from the Ministry of Foreign Affairs of Lithuania, dated 26 April 2004, registered**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	at the Secretariat General on 10 May 2004 - Or. Engl. Pursuant to Article 40 and Article 27, paragraph 9, sub-paragraph e, of the Convention, the Republic of Lithuania declares that, for reasons of efficiency, requests for mutual assistance made under Article 27, paragraph 9, are to be addressed to the above-designated central authorities. **Period covered: 1/7/2004 -** The preceding statement concerns Article(s) : 27 **Reservation contained in the instrument of ratification deposited on 18 March 2004 - Or. Engl. - and confirmed by a Note verbale from the Ministry of Foreign Affairs of Lithuania, dated 26 April 2004, registered at the Secretariat General on 10 May 2004 - Or. Engl.** In accordance with Article 42 and Article 4, pararaph 2, of the Convention, the Republic of Lithuania declares that criminal liability occurs if the acts described in Article 4 of the Convention result in serious harm. **Period covered: 1/7/2004 -** The preceding statement concerns Article(s) : 4 **Reservation contained in the instrument of ratification deposited on 18 March 2004 - Or. Engl. - and confirmed by a Note verbale from the Ministry of Foreign Affairs of Lithuania, dated 26 April 2004, registered at the Secretariat General on 10 May 2004 - Or. Engl.** In accordance with Article 42 and Article 29, pararaph 4, of the Convention, the Republic of Lithuania declares that it reserves the right to refuse to execute the request for preservation of the data in cases where there is reason to believe that at the time of disclosure the offence, on which the request for preservation of the data is based, is not considered as a crime by the laws of the Republic of Lithuania.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Period covered: 1/7/2004 - The preceding statement concerns Article(s) : 29 **Declaration contained in the instrument of ratification deposited on 18 March 2004 - Or. Engl. - and confirmed by a Note verbale from the Ministry of Foreign Affairs of Lithuania, dated 26 April 2004, registered at the Secretariat General on 10 May 2004 - Or. Engl.** Pursuant to Article 24, paragraph 7, sub-paragraph a, of the Convention, the Republic of Lithuania declares that the Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania are designated as responsible authorities to perform the functions mentioned in Article 24, paragraph 7, sub-paragraph a. **Period covered: 1/7/2004 -** The preceding statement concerns Article(s) : 24 **Declaration contained in the instrument of ratification deposited on 18 March 2004 - Or. Engl. - and confirmed by a Note verbale from the Ministry of Foreign Affairs of Lithuania, dated 26 April 2004, registered at the Secretariat General on 10 May 2004 - Or. Engl.** Pursuant to Article 27, paragraph 2, sub-paragraph a, of the Convention, the Republic of Lithuania declares that the Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania are designated as central authorities to perform the functions mentioned in Article 27. **Period covered: 1/7/2004 -** The preceding statement concerns Article(s) : 27 **Declaration contained in the instrument of ratification deposited on 18 March 2004 - Or. Engl. - and confirmed by a Note verbale from the Ministry of Foreign Affairs of Lithuania, dated 26 April 2004, registered**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	at the Secretariat General on 10 May 2004 - Or. Engl. Pursuant to Article 35, paragraph 1, of the Convention, the Republic of Lithuania declares that the Police Department under the Ministry of the Interior of the Republic of Lithuania is designated as a competent authority to perform the functions mentioned in Article 35. **Period covered: 1/7/2004 -** The preceding statement concerns Article(s) : 35

Back to the Table of Contents