Estonia

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 15 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:	23/11/2001
Ratification/accession:	12/05/2003

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	The definitions from the Convention are directly applicable for Estonia.
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	**§ 217. Illegal obtaining of access to computer systems**

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) Illegal obtaining of access to computer systems by elimination or avoidance of means of protection is punishable by a pecuniary punishment or up to three years' imprisonment. (2) The same act: 1) if it causes significant damage; or 2) if access was obtained to a computer system containing a state secret, classified foreign information or information prescribed for official use only; or 3) if access was obtained to a computer system of a vital sector, is punishable by a pecuniary punishment or up to five years' imprisonment. (3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.
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.	**§ 137. Unauthorised surveillance** (1) Observation of another person in order to collect information relating to such person by a person without the lawful right to engage in surveillance is punishable by a pecuniary punishment or up to three years' imprisonment. (2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
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.	**§ 206. Interference with computer data** (1) Illegal alteration, deletion, damaging or blocking of data in computer systems is punishable by a pecuniary punishment or up to three years' imprisonment. (2) The same act if: 1) committed against data in numerous computer systems and the devices or computer programs specified in § 216^1 of this Code were used for the commission thereof; 2) committed by a group; 3) committed against data in a computer system of a vital sector; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	4) it causes significant damage; is punishable by a pecuniary punishment or up to five years' imprisonment. (3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.
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	**§ 207. Hindering of functioning of computer systems** (1) Illegal interference with or hindering of the functioning of computer systems by way of uploading, transmitting, deleting, damaging, altering or blocking of data is punishable by a pecuniary punishment or up to three years' imprisonment. (2) The same act if: 1) committed against numerous computer systems and the devices or computer programs specified in § 216[1] of this Code were used for the commission thereof; 2) committed by a group; 3) the functioning of a computer system of a vital sector or the provision of public services is interfered or hindered thereby; or 4) it causes significant damage, is punishable by a pecuniary punishment or up to five years' imprisonment. (3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.
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	**§ 216[1]. Preparation of computer-related crime** (1) Supply, production, possession, distribution or making otherwise available of a device or computer program which is created or adjusted in particular for the commission of the criminal offences provided for in §§ 206, 207, 213 or 217 of this Code, or of the means of protection which allow to get access to a computer system with the intention of committing himself or herself or enabling a third person to commit the crimes provided for in §§ 206, 207, 213 or 217 of this Code is punishable by a pecuniary punishment or up to two years' imprisonment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment. (3) A court may, pursuant to the provisions of § 83 of this Code, apply confiscation of an object which was the direct object of the commission of an offence provided for in this section.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**§ 344.** Counterfeiting of documents, seals or blank document forms (1) Counterfeiting a document, seal or blank document form on the basis of which it is possible to obtain rights or release from obligations is punishable by a pecuniary punishment or up to one year of imprisonment. (2) The same act, if committed by a legal person, is punishable by a pecuniary punishment. **§ 345.** Use of counterfeit documents, seals or blank document forms (1) Use of a knowingly counterfeit document, seal or blank document form with the intention of obtaining rights or release from obligations is punishable by a pecuniary punishment or up to three years' imprisonment. [RT I, 12.07.2014, 1 - entry into force 01.01.2015] (2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	§ 347. Falsification of important identity documents (1) Falsification of an important identity document is punishable by a pecuniary punishment or up to three years' imprisonment. [RT I, 12.07.2014, 1 - entry into force 01.01.2015] (2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
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.	**§ 213. Computer-related fraud** (1) Causing of proprietary damage to another person through unlawful entry, alteration, deletion, damaging or blocking of computer programs or data or other unlawful interference with data processing operation for the purpose of proprietary benefit is punishable by a pecuniary punishment or up to three years' imprisonment. (2) The same act, if committed: 1) by a person who has previously committed theft, robbery, embezzlement, acquisition, storage or marketing of property received through commission of an offence, intentional damaging or destruction of a thing, fraud or extortion; 2) by an official; 3) on a large-scale basis; or 4) by a group, is punishable by one to five years' imprisonment. (3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.
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	**§ 175[1]. Requesting access to child pornography and watching thereof** (1) Knowingly requesting access to child pornography or knowingly watching a pornographic performance involving a person younger than eighteen years of age or of a pornographic or erotic performance involving a person younger than fourteen years of age is punishable by a pecuniary punishment or up to two

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	years' imprisonment. (2) The same act, if committed by a person who has previously committed a criminal offence provided for in this section or §§ 175 or 178 to 179, is punishable by up to three years' imprisonment. (3) The same act, if committed by a legal person, is punishable by a pecuniary punishment. **§ 178. Manufacture of works involving child pornography or making child pornography available** (1) Manufacture, acquisition or storing, handing over, displaying or making available to another person in any other manner of pictures, writings or other works or reproductions of works depicting a person of less than eighteen years of age in a pornographic situation, or a person of less than fourteen years of age in a pornographic or erotic situation, is punishable by a pecuniary punishment or up to three years' imprisonment. (1[1]) The same act if committed by a person who has previously committed a criminal offence provided for in this section or §§ 175, 175[1], 178[1] or 179 is punishable by one to three years' imprisonment. (2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
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	**§ 222[1]. Infringement of copyright in computer system** (1) Knowing infringement of proprietary rights of a holder of copyright or related rights by means of a computer system in professional or economic activities, if the amount of gains or damage caused by the infringement exceeds the amount of twenty minimum daily rates and it does not contain the necessary elements provided for in § 222, is punishable by a pecuniary

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	punishment or up to one year of imprisonment. (2) The same act, if committed by a legal person, is punishable by a pecuniary punishment. (3) The court shall confiscate the object which was the direct object of commission of an offence provided for in this section.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**§ 25. Attempt** (1) An attempt is an intentional act the purpose of which is to commit an offence. (2) An attempt is deemed to have commenced at the moment when the person, according to the person's understanding of the act, directly commences the commission of the offence. (3) If an act is committed by taking advantage of another person, the attempt is deemed to have commenced at the moment when the person loses control over the events or when the intermediary directly commences the commission of the offence according to the person's understanding of the act. (4) In the case of a joint offence, the attempt is deemed to have commenced at the moment when at least one of the persons directly commences the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	commission of the offence according to the agreement of the persons. (5) In the case of an omission, the attempt is deemed to have commenced at the moment when the person fails to perform an act which is necessary for the prevention of the consequences which constitute the necessary elements of an offence. (6) In the case of an attempt, the court may apply the provisions of § 60 of this Code. **§ 22. Accomplice** (1) Accomplices are abettors and aiders. (2) An abettor is a person who intentionally induces another person to commit an intentional unlawful act. (3) An aider is a person who intentionally provides physical, material or moral assistance to an intentional unlawful act of another person. (4) Unless otherwise provided for in § 24 of this Code, a punishment shall be imposed on an accomplice pursuant to the same provision of law which prescribes the liability of the principal offender. (5) In the case of an aider, the court may apply the provisions of § 60 of this Code.
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.	**§ 14. Liability of legal person** (1) In the cases provided by law, a legal person shall be held responsible for an act which is committed in the interests of the legal person by its body, a member thereof or by a senior official or competent representative. (2) Prosecution of a legal person does not preclude prosecution of the natural

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	person who committed the offence. (3) The provisions of this section do not apply to the state, international organisations, local governments or to legal persons in public law.
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the 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.	**§ 32. Investigative bodies in criminal procedure** (1) An investigative body shall perform the procedural acts provided in this Code independently unless the permission of a court or the permission or order of the Prosecutor's Office is necessary for the performance of the act. (2) An investigative body has the right to demand submission of any document necessary for solving a criminal matter. **§ 215. Obligation to comply with orders and demands of investigative bodies and prosecutors' offices** (1) The orders and demands issued by investigative bodies and prosecutors' offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia. The orders and demands issued by investigative bodies and prosecutor's offices are binding on the members of Defence Forces engaged in missions abroad, if the object of the criminal proceeding is an act of a person serving in the Defence Forces. Costs incurred for compliance with a claim or ruling shall not be compensated for. (2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately. (3) A preliminary investigation judge may impose a fine on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a prosecutor's office. The suspect and accused shall not be fined.
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	**§ 32. Investigative bodies in criminal procedure** (1) An investigative body shall perform the procedural acts provided in this Code independently unless the permission of a court or the permission or order of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Prosecutor's Office is necessary for the performance of the act. (2) An investigative body has the right to demand submission of any document necessary for solving a criminal matter **§ 215. Obligation to comply with orders and demands of investigative bodies and prosecutors' offices** (1) The orders and demands issued by investigative bodies and prosecutors' offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia. The orders and demands issued by investigative bodies and prosecutor's offices are binding on the members of Defence Forces engaged in missions abroad, if the object of the criminal proceeding is an act of a person serving in the Defence Forces. Costs incurred for compliance with a claim or ruling shall not be compensated for. (2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately. (3) A preliminary investigation judge may impose a fine on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a prosecutor's office. The suspect and accused shall not be fined. **ECA § 111[1]. Obligation to preserve data** (1) A communications undertaking is required to preserve the data that are necessary for the performance of the following acts: 1) tracing and identification of the source of communication; 2) identification of the destination of communication; 3) identification of the date, time and duration of communication; 4) identification of the type of communications service; 5) identification of the terminal equipment or presumable terminal equipment of a user of communications services; 6) determining of the location of the terminal equipment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data: 1) the number of the caller and the subscriber's name and address; 2) the number of the recipient and the subscriber's name and address; 3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address; 4) the date and time of the beginning and end of the call; 5) the telephone or mobile telephone service used; 6) the international mobile subscriber identity (*IMSI*) of the caller and the recipient; 7) the international mobile equipment identity (*IMEI*) of the caller and the recipient; 8) the cell ID at the time of setting up the call; 9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved; 10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated. (3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data: 1) the user IDs allocated by the communications undertaking; 2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network; 3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication; 4) the user ID or telephone number of the intended recipient of an Internet telephony call; 5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services; 6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID; 7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone; 8) the Internet service used in the case of electronic mail and Internet telephony services; 9) the number of the caller in the case of dial-up Internet access; 10) the digital subscriber line (*DSL*) or other end point of the originator of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	communication. (4) The data specified in subsections (2) and (3) of this section shall be preserved for one year from the date of the communication if such data are generated or processed in the process of provision of communications services. Requests submitted and information given pursuant to § 112 of this Act shall be preserved for two years. The obligation to preserve the information provided pursuant to § 112 rests with the person submitting the request. (5) The data specified in subsections (2) and (3) of this section shall be preserved in the territory of a Member State of the European Union. The following shall be preserved in the territory of Estonia: 1) the requests and information provided for in § 112 of this Act; 2) the log files specified in subsection 113 (5) and the applications provided for in subsection 113 (6) of this Act; 3) the single requests provided for in § 114[1] of this Act. (6) In the interest of public order and national security the Government of the Republic may extend, for a limited period, the term specified in subsection (4) of this section. (7) In the case specified in subsection (6) of this section the minister responsible for the area shall immediately notify the European Commission and the Member States of the European Union thereof. In the absence of an opinion of the European Commission within a period of six months the term specified in subsection (4) shall be deemed to have been extended. (8) The obligation to preserve the data provided for in subsections (2) and (3) of this section also applies to unsuccessful calls if those data are generated or processed upon providing telephone or mobile telephone services or telephone network or mobile telephone network services. The specified obligation to preserve data does not apply to call attempts. (9) Upon preserving the data specified in subsections (2) and (3) of this section, a communications undertaking must ensure that: 1) the same quality, security and data protection requirements are met as those applicable to analogous data on the electronic communications network; 2) the data are protected against accidental or unlawful destruction, loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	3) necessary technical and organisational measures are in place to restrict access to the data; 4) no data revealing the content of the communication are preserved. (10) The expenses related to the preserving or processing of the data specified in subsections (2) and (3) of this section shall not be compensated to communications undertakings. (11) The data specified in subsections (2) and (3) of this section are forwarded to: 1) an investigative body, a surveillance agency, the Prosecutor's Office or a court pursuant to the Code of Criminal Procedure; 2) a security authority; 3) the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Security Police Board and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure; 4) the Financial Supervision Authority pursuant to the Securities Market Act; 5) a court pursuant to the Code of Civil Procedure; 6) a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act and the Aliens Act. **ECA § 112. Obligation to provide information** (1) If an agency or authority specified in subsection 111^1 (11) of this Act submits a request, a communications undertaking is required to provide at the earliest opportunity, but not later than ten hours after receiving an urgent request or within ten working days after receipt of the request if the request is not urgent, if adherence to the specified terms is possible based on the substance of the request, the agency or authority with information concerning the data specified in subsections 111^1 (2) and (3) of this Act. (2) A request specified in subsection (1) of this section shall be submitted in writing or by electronic means. Requests concerning the data specified in clauses 111^1 (2) 1) and 2) and (3) 3) of the Act may also be submitted in oral form confirming the request with a password. Access to the data specified in subsection (1) of this section may be ensured, on the basis of a written

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	contract, by way of continuous electronic connection. (3) A communications undertaking providing mobile telephone services is required to provide a surveillance agency and security authority and the Police and Border Guard Board on the bases provided for in the Police and Border Guard Act with real time identification of the location of the terminal equipment used in the mobile telephone network. (4) Access to the data specified in subsection (3) of this section must be ensured on the basis of a written contract and by way of continuous electronic connection.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service	**§ 32. Investigative bodies in criminal procedure** (1) An investigative body shall perform the procedural acts provided in this Code independently unless the permission of a court or the permission or order of the Prosecutor's Office is necessary for the performance of the act. (2) An investigative body has the right to demand submission of any document necessary for solving a criminal matter **§ 215. Obligation to comply with orders and demands of investigative bodies and prosecutors' offices** (1) The orders and demands issued by investigative bodies and prosecutors' offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia. The orders and demands issued by investigative bodies and prosecutor's offices are binding on the members of Defence Forces engaged in missions abroad, if the object of the criminal proceeding is an act of a person serving in the Defence Forces. Costs incurred for compliance with a claim or ruling shall not be compensated for. (2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
agreement or arrangement.	bodies shall be complied with immediately. (3) A preliminary investigation judge may impose a fine on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a prosecutor's office. The suspect and accused shall not be fined. **§ 90[1]. Request to electronic communications undertakings to submit information** (1) A body conducting proceedings may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of communication of messages. (2) With the permission of a prosecutor's office an investigative body may make enquiries in pre-trial procedure or with the permission of a court in court proceeding to electronic communications undertakings about the data listed in subsections 111[1] (2) and (3) of the Electronic Communications Act and not specified in the first subsection of this section. The permission to make inquiries shall set out the dates of the period of time about which the requesting of data is permitted. (3) The enquiries prescribed in this section may be made only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings. **ECA § 102. General principles of data protection** (1) A communications undertaking is required to maintain the confidentiality of all information which becomes known thereto in the process of provision of communications services and which concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber; above all, it must maintain the confidentiality of: 1) information concerning specific details related to the use of communications services;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2) the content and format of messages transmitted over the communications network; 3) information concerning the time and manner of transmission of messages. (2) The information specified in subsection (1) of this section may be disclosed only to the relevant subscriber and, with the consent of the subscriber, to third persons, except in the cases specified in §§ 112, 113 and 114[1] of this Act. A subscriber has the right to withdraw his or her consent at any time. (3) A communications undertaking may process the information provided for in subsection (1) of this section if the undertaking notifies the subscriber, in a clear and unambiguous manner, of the purposes of processing the information and gives the subscriber an opportunity to refuse the processing. (4) The obligation of a communications undertaking specified in subsection (3) of this section does not restrict the right of the undertaking to collect and process, without the consent of a subscriber, information which processing is necessary for the purposes of recording the transactions made in the course of business and for other business-related exchange of information. In addition to the above, the restriction provided for in subsection (3) of this section does not limit the right of a communications undertaking to store or process information without the consent of a subscriber if the sole purpose thereof is the provision of services over the communications network, or if it is necessary for the provision, upon a direct request of the subscriber, of information society services within the meaning of the Information Society Services Act. **ECA § 111[1]. Obligation to preserve data** (1) A communications undertaking is required to preserve the data that are necessary for the performance of the following acts: 1) tracing and identification of the source of communication; 2) identification of the destination of communication; 3) identification of the date, time and duration of communication; 4) identification of the type of communications service; 5) identification of the terminal equipment or presumable terminal equipment of a user of communications services; 6) determining of the location of the terminal equipment. (2) The providers of telephone or mobile telephone services and telephone

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	network and mobile telephone network services are required to preserve the following data: 1) the number of the caller and the subscriber's name and address; 2) the number of the recipient and the subscriber's name and address; 3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialed and the subscriber's name and address; 4) the date and time of the beginning and end of the call; 5) the telephone or mobile telephone service used; 6) the international mobile subscriber identity (*IMSI*) of the caller and the recipient; 7) the international mobile equipment identity (*IMEI*) of the caller and the recipient; 8) the cell ID at the time of setting up the call; 9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved; 10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated. (3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data: 1) the user IDs allocated by the communications undertaking; 2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network; 3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication; 4) the user ID or telephone number of the intended recipient of an Internet telephony call; 5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services; 6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID; 7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone; 8) the Internet service used in the case of electronic mail and Internet telephony services; 9) the number of the caller in the case of dial-up Internet access; 10) the digital subscriber line (*DSL*) or other end point of the originator of the communication.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) The data specified in subsections (2) and (3) of this section shall be preserved for one year from the date of the communication if such data are generated or processed in the process of provision of communications services. Requests submitted and information given pursuant to § 112 of this Act shall be preserved for two years. The obligation to preserve the information provided pursuant to § 112 rests with the person submitting the request. (5) The data specified in subsections (2) and (3) of this section shall be preserved in the territory of a Member State of the European Union. The following shall be preserved in the territory of Estonia: 1) the requests and information provided for in § 112 of this Act; 2) the log files specified in subsection 113 (5) and the applications provided for in subsection 113 (6) of this Act; 3) the single requests provided for in § 114[1] of this Act. (6) In the interest of public order and national security the Government of the Republic may extend, for a limited period, the term specified in subsection (4) of this section. (7) In the case specified in subsection (6) of this section the minister responsible for the area shall immediately notify the European Commission and the Member States of the European Union thereof. In the absence of an opinion of the European Commission within a period of six months the term specified in subsection (4) shall be deemed to have been extended. (8) The obligation to preserve the data provided for in subsections (2) and (3) of this section also applies to unsuccessful calls if those data are generated or processed upon providing telephone or mobile telephone services or telephone network or mobile telephone network services. The specified obligation to preserve data does not apply to call attempts. (9) Upon preserving the data specified in subsections (2) and (3) of this section, a communications undertaking must ensure that: 1) the same quality, security and data protection requirements are met as those applicable to analogous data on the electronic communications network; 2) the data are protected against accidental or unlawful destruction, loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	3) necessary technical and organisational measures are in place to restrict access to the data; 4) no data revealing the content of the communication are preserved. (10) The expenses related to the preserving or processing of the data specified in subsections (2) and (3) of this section shall not be compensated to communications undertakings. (11) The data specified in subsections (2) and (3) of this section are forwarded to: 1) an investigative body, a surveillance agency, the Prosecutor's Office or a court pursuant to the Code of Criminal Procedure; 2) a security authority; 3) the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Security Police Board and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure; 4) the Financial Supervision Authority pursuant to the Securities Market Act; 5) a court pursuant to the Code of Civil Procedure; 6) a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act and the Aliens Act. **ECA § 112. Obligation to provide information** (1) If an agency or authority specified in subsection 111^1 (11) of this Act submits a request, a communications undertaking is required to provide at the earliest opportunity, but not later than ten hours after receiving an urgent request or within ten working days after receipt of the request if the request is not urgent, if adherence to the specified terms is possible based on the substance of the request, the agency or authority with information concerning the data specified in subsections 111^1 (2) and (3) of this Act. (2) A request specified in subsection (1) of this section shall be submitted in writing or by electronic means. Requests concerning the data specified in clauses 111^1 (2) 1) and 2) and (3) 3) of the Act may also be submitted in oral form confirming the request with a password. Access to the data specified in subsection (1) of this section may be ensured, on the basis of a written

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	contract, by way of continuous electronic connection. (3) A communications undertaking providing mobile telephone services is required to provide a surveillance agency and security authority and the Police and Border Guard Board on the bases provided for in the Police and Border Guard Act with real time identification of the location of the terminal equipment used in the mobile telephone network. (4) Access to the data specified in subsection (3) of this section must be ensured on the basis of a written contract and by way of continuous electronic connection.
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;	**§ 91. Search** (1) The objective of a search is to find an object to be confiscated or used as physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, assets to be seized in criminal proceedings, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area. A search may be conducted if there is reasonable doubt that the object to be found is at the place of the search. (2) Unless otherwise provided by this Code, a search may be conducted at the request of a prosecutor's office on the basis of an order of a preliminary investigation judge or on the basis of a court ruling. Both an order of a preliminary investigation judge as well as a court ruling on the adjudication of a search request of a prosecutor's office may be drawn up as an inscription on the request of a prosecutor's office. (3) A search may be conducted on the basis of an order of a prosecutor's office, except for searches of a notary's office or advocate's law office or at the persons processing information for journalistic purposes, if there is reason to believe that the suspect used or uses the site or vehicle to be searched at the time of commission of a criminal act or during the pre-trial proceedings, and the person is suspected of committing the crime specified in subsection 126^2 (2) of this

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Code. (4) A search warrant shall set out: 1) what is being searched for as the objective of the search (hereinafter *object to be found*); 2) the reasons for the search; 3) the place where the search is conducted. (5) In the cases of urgency, if execution of a search warrant on time is impossible, a search may be conducted on the terms and conditions specified in subsection (3) of this section on the basis of an authorisation of the prosecutor's office issued in a format which can be reproduced in writing. (6) When a search is conducted on the bases specified in subsections (3) and (5) of this section, a preliminary investigation judge has to be notified thereof through a prosecutor's office during the first working day following the beginning of the search. A preliminary investigation judge shall decide on the admissibility of the search by a ruling which may be drawn up as an inscription on the ruling of the prosecutor's office. (7) If a search is conducted, the search warrant shall be presented for examination to the person whose premises are to be searched or to his or her adult family member or a representative of the legal person or the state or local government agency whose premises are to be searched. The ruling shall be signed to confirm the presentation. In the case specified in subsection (5) of this section, the person whose premises are to be searched or his or her adult family member or a representative of the legal person or the state of local government agency whose premises are to be searched shall be explained upon implementation of a search the circumstances specified in subsections (4) of this section and the reasons for conducting a search urgently. The search report shall be signed to confirm that explanations of the circumstances were provided. In the absence of the responsible person or representative, a representative of the local government shall be involved. (8) A notary's office or an advocate's law office shall be searched in the presence of the notary or advocate. If the notary or advocate cannot be present during the search, the search shall be conducted in the presence of a person substituting for the notary or another advocate providing legal services through

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the same law office, or if this is impossible, another notary or advocate. (9) When a search is implemented, the person shall be asked to hand over the object to be found or to show where the body is hidden or the fugitive is hiding. If the proposal is not complied with or if there is reason to believe that the person complied with the proposal only partly, a search shall be conducted. (10) In the course of a search, all objects may be taken away which are subject to confiscation or are evidently the evidence in the criminal proceedings if they were discovered without any search in a clearly visible place or in the course of reasonable search undertaken to find the objects to be found. **§ 126^3. Surveillance activities** (1) On the basis specified in subsection 126^2 (1) of this Code, a surveillance agency may covertly watch a person, thing or area, covertly take comparative samples and perform initial examinations, covertly examine a thing and covertly replace it. (2) The Police and Border Guard Board and the Security Police Board may conduct the following surveillance activities on the basis specified in clause 126^2 (1) 1) of this Code upon collection of information concerning the preparation for the criminal offence specified in §§ 244 and 246, clause 266 (2) 3) and §§ 255 and 256 of the Penal Code and on the basis specified in clauses 3) and 4): 1) to covertly examine a postal item; 2) to covertly observe or wire-tap information; 3) to use a police agent. (3) The Police and Border Guard Board and the Security Police Board may stage a criminal offence on the basis specified in clause 126^2 (1) 4) of this Code for the purpose of detection of a criminal offence or detention of a criminal. (4) The Prisons Department of the Ministry of Justice and prisons may conduct the following surveillance activities specified in clauses 126^2 (1) 1) and 4) of this Code: 1) to covertly examine a postal item; 2) to covertly observe or wire-tap information. (5) Covert entry into a building, premises, vehicle, enclosed area or computer

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	system is permitted upon conduct of the surveillance activities specified in subsection (1) and clauses (2) 2) and 3) of this section in the case this is unavoidably necessary for the achievement of the objectives of the surveillance activities. (6) For the purposes of this Act, entry into the possessions of other persons is deemed to be covert if the fact of entry is covert for the possessor or if a misconception of existing facts is knowingly caused by fraud upon entry and the possessor, with knowledge of the actual circumstances, would not have given possession for entry. **§ 126[5]. Covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things** (1) A prosecutor's office shall issue a permission for covert surveillance of persons, things or areas, covert collection of comparative samples and conduct of initial examinations and covert examination or replacement of things for up to two months. The prosecutor's office may extend the term of the permission for up to two months at a time. (2) In the course of the surveillance activities specified in this section, the information collected shall be, if necessary, video recorded, photographed or copied or recorded in another way.
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.	**§ 126[7]. Wire-tapping or covert observation of information** (1) Information obtained by wire-tapping or covert observation of messages or other information transmitted by the public electronic communications network or communicated by any other means shall be recorded. (2) Information communicated by a person specified in § 72 of this Code or information communicated to such person by another person which is subject to wire-tapping or covert observation shall not be used as evidence if such information contains facts which have become known to the person in his or her professional activities, unless: 1) the person specified in § 72 of this Code has already given testimony with regard to the same facts or if the facts have been disclosed in any other manner; 2) a permission has been granted with respect to such person for wire-tapping

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	or covert observation; or 3) it is evident on the basis of wire-tapping or covert observation of another person that the specified person commits or has committed a criminal offence. (3) A preliminary investigation judge grants permission for the surveillance activities specified in this section for up to two months. After expiry of the specified term, the preliminary investigation judge may extent this term by up to two months.
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.	**§ 126[7]. Wire-tapping or covert observation of information** (1) Information obtained by wire-tapping or covert observation of messages or other information transmitted by the public electronic communications network or communicated by any other means shall be recorded. (2) Information communicated by a person specified in § 72 of this Code or information communicated to such person by another person which is subject to wire-tapping or covert observation shall not be used as evidence if such information contains facts which have become known to the person in his or her professional activities, unless: 1) the person specified in § 72 of this Code has already given testimony with regard to the same facts or if the facts have been disclosed in any other manner; 2) a permission has been granted with respect to such person for wire-tapping or covert observation; or 3) it is evident on the basis of wire-tapping or covert observation of another person that the specified person commits or has committed a criminal offence. (3) A preliminary investigation judge grants permission for the surveillance activities specified in this section for up to two months. After expiry of the specified term, the preliminary investigation judge may extent this term by up to two months.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 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.	**§ 6. Territorial applicability of penal law** (1) The penal law of Estonia applies to acts committed within the territory of Estonia. (2) The penal law of Estonia applies to acts committed on board of or against ships or aircraft registered in Estonia, regardless of the location of the ship or aircraft at the time of commission of the offence or the penal law of the country where the offence is committed. **§ 7. Applicability of penal law by reason of person concerned** (1) The penal law of Estonia applies to an act committed outside the territory of Estonia if such act constitutes a criminal offence pursuant to the penal law of Estonia and is punishable at the place of commission of the act, or if no penal power is applicable at the place of commission of the act and if: 1) the act is committed against a citizen of Estonia or a legal person registered in Estonia; or 2) the offender is a citizen of Estonia at the time of commission of the act or becomes a citizen of Estonia after the commission of the act, or if the offender is an alien who has been detained in Estonia and is not extradited. (2) The penal law of Estonia applies: 1) to an act committed outside the territory of Estonia if such act constitutes a criminal offence pursuant to the penal law of Estonia and the offender is a member of the Defence Forces performing his or her duties; 2) to grant, acceptance or arranging receipt of gratuities or bribes or influence peddling committed outside the territory of Estonia if such act was committed by an Estonian citizen, Estonian official or a legal person registered in Estonia, or an alien who has been detained in Estonia and who is not extradited, or such person participated therein. **§ 8. Applicability of penal law to acts against internationally protected**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	legal rights Regardless of the law of the place of commission of an act, the penal law of Estonia shall apply to any acts committed outside the territory of Estonia if punishability of the act arises from an international obligations binding on Estonia. **§ 9. Applicability of penal law to acts against legal rights of Estonia** (1) Regardless of the law of the place of commission of an act, the penal law of Estonia applies to acts committed outside the territory of Estonia if according to the penal law of Estonia the act is a criminal offence in the first degree and if such act: 1) causes damage to the life or health of the population of Estonia; 2) interferes with the exercise of state authority or the defence capability of Estonia; or 3) causes damage to the environment. (2) Regardless of the type of the offence, the penal law of Estonia applies to acts, which damage the environment and were committed within the economic zone or on the high seas, in accordance with the requirements and rights of international maritime law established with respect to foreign vessels.
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	**§ 438. Admissibility of extradition** Estonia as the executing state is entitled to extradite a person on the basis of a request for extradition if criminal proceedings have been initiated and an arrest warrant has been issued with regard to the person in the requesting state or if the person has been sentenced to imprisonment by a judgment of conviction which has entered into force. **§ 439. General conditions for extradition of persons to foreign states**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	(1) Extradition of a person for the purposes of continuation of the criminal proceedings concerning him or her in a foreign state is permitted if the person is suspected or accused of a criminal offence which is punishable by at least one year of imprisonment according to both the penal law of the requesting state and the Penal Code of Estonia. (2) Extradition of a person for the purposes of execution of a judgment of conviction made with regard to him or her is permitted under the conditions provided for in subsection (1) of this section if at least four months of the sentence of imprisonment have not yet been served. (3) If a person whose extradition is requested has committed several criminal offences and extradition is permitted for some of the criminal offences, extradition may be granted also for the other offences which do not meet the requirements specified in subsections (1) and (2) of this section.
Article 25 – General principles relating to mutual assistance	**§ 433. General principles**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 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.	(1) International cooperation in criminal procedure comprises extradition of persons to foreign states, mutual assistance between states in criminal matters, execution of the judgments of foreign courts, taking over and transfer of criminal proceedings commenced, cooperation with the International Criminal Court and Eurojust and extradition to Member States of the European Union. (2) International cooperation in criminal procedure shall be effected pursuant to the provisions of this Chapter unless otherwise prescribed by the international agreements of the Republic of Estonia, the European Union legislation or the generally recognised principles of international law. (3) International cooperation in criminal procedure shall be effected pursuant to the provisions of the other chapters of this Code in so far as this is not in conflict with the provisions of this Chapter. (4) If adherence to the requirement of confidentiality is requested in the course of international cooperation in criminal procedure, such requirement shall be complied with to the extent necessary for the purposes of cooperation. If compliance with the confidentiality requirement is refused, the requesting state shall be immediately notified of such refusal. **§ 435. Judicial authorities competent to engage in international cooperation in criminal procedure** (1) The central authority for international cooperation in criminal procedure is the Ministry of Justice, unless otherwise provided by law or international legislation binding on the Republic of Estonia. (2) Courts, the prosecutors' offices, the Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Environmental Inspectorate, the Competition Board and the Military Police are the judicial authorities competent to engage in international cooperation in criminal procedure to the extent provided by law and international legislation binding on the Republic of Estonia. (3) If the Penal Code of Estonia is applied to criminal offences which are committed outside the territory of the Republic of Estonia, the Office of the Prosecutor General, which initiates criminal proceedings or verifies the legality

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and justification of commencement of the criminal proceedings, shall be immediately informed thereof. **§ 462. Processing of requests for assistance received from foreign states** (1) The Ministry of Justice shall verify whether a request for assistance received from a foreign state meets the requirements. A request for assistance in compliance with the requirements shall be immediately communicated to the Office of the Prosecutor General. (2) The Office of the Prosecutor General shall verify whether compliance with the request for assistance is admissible and possible and communicate the request for assistance to the competent judicial authority for execution. (3) Requests for assistance received by investigative bodies shall be communicated to the Office of the Prosecutor General. In cases of urgency, a request for assistance submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may be complied with before the request for assistance is received by the Ministry of Justice with the consent of the Office of the Prosecutor General. **§ 463. Compliance with requests for assistance received from foreign states** (1) Requests for assistance are complied with pursuant to this Code. At the request of a foreign state, a request may be complied with pursuant to procedural provisions different from the provisions of this Code unless this is contrary to the principles of Estonian law. (1^1) If summoning of a person to court is required for compliance with a request for assistance, service of the summons shall be organised by the court. (2) The materials received as a result of compliance with a request shall be communicated to the requesting state using the same channel which was used for sending the request, except in the case the requesting state requests the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	sending of the materials directly to the initiator of the request. (2[1]) If it becomes evident upon compliance with a request that is expedient to perform additional acts which were not requested, the requesting state shall be notified thereof. (3) The materials received as a result of compliance with a request for assistance from a foreign state submitted through Eurojust shall be sent to the requesting state through Eurojust unless otherwise agreed with Eurojust.
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.	**§ 473. Spontaneous exchange of information** Within the framework of mutual assistance in criminal procedure, a competent judicial authority may forward to a foreign state and, in the case of criminal offences listed in subsection 491 (2) of this Code, to Eurojust information obtained by a procedural act performed without prior request when such information may be the reason for initiating a criminal proceeding in such foreign state or may assist in ascertaining the facts relating to a criminal offence subject to a criminal proceeding already initiated.
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	

Back to the Table of Contents

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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 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	See § 433. General principles above

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; 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:	**§ 464.** Submission of requests for assistance to foreign states (1) Unless otherwise prescribed by an international agreement entered into by the Republic of Estonia, a request for assistance shall be submitted to the Public Prosecutor's Office which shall verify whether the request meets the requirements. The Public Prosecutor's Office shall forward requests in compliance with the requirements to the Ministry of Justice. (2) The Ministry of Justice shall immediately make a decision on the submission of or refusal to submit a request to a foreign state and notify the judicial authority which submitted the request of such decision. Refusal to submit a request shall be reasoned. (3) In cases of urgency, a request may be submitted also through the International Criminal Police Organisation (Interpol) and communicated concurrently through the judicial authorities specified in subsection (1) of this section. The central authority responsible for the national section of the Schengen Information System has the right to add a notice in the Schengen Information System before preparing a request for assistance in order to ensure application of a measure necessary for compliance with the request for assistance. [RT I, 23.02.2011, 1 - entry into force 01.09.2011] (4) If the protection of a witness is requested, the measures of protection shall be agreed upon separately. [RT I 2008, 19, 132 - entry into force 23.05.2008] (5) In cases of urgency, a request for assistance in criminal offences listed in subsection 491 (2) of this Code may be submitted to a Member State of the European Union through Eurojust. [RT I 2008, 19, 132 - entry into force 23.05.2008] (6) In cases of urgency, Eurojust's National Member for Estonia may prepare a request for assistance in a criminal offence the proceeding of which is to be conducted in Estonia and submit it to a foreign state. [RT I 2008, 19, 132 - entry into force 23.05.2008] (7) The following are competent to submit a request for assistance to foreign states: 1) in pre-trial proceedings, the prosecutor conducting the proceedings; 2) in matters which are subject to court proceedings, the court.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	[RT I 2008, 19, 132 - entry into force 23.05.2008]
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.	**§ 464.** Submission of requests for assistance to foreign states (1) Unless otherwise prescribed by an international agreement entered into by the Republic of Estonia, a request for assistance shall be submitted to the Public Prosecutor's Office which shall verify whether the request meets the requirements. The Public Prosecutor's Office shall forward requests in compliance with the requirements to the Ministry of Justice. (2) The Ministry of Justice shall immediately make a decision on the submission of or refusal to submit a request to a foreign state and notify the judicial authority which submitted the request of such decision. Refusal to submit a request shall be reasoned. (3) In cases of urgency, a request may be submitted also through the International Criminal Police Organisation (Interpol) and communicated concurrently through the judicial authorities specified in subsection (1) of this section. The central authority responsible for the national section of the Schengen Information System has the right to add a notice in the Schengen Information System before preparing a request for assistance in order to ensure application of a measure necessary for compliance with the request for assistance. [RT I, 23.02.2011, 1 - entry into force 01.09.2011] (4) If the protection of a witness is requested, the measures of protection shall

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	be agreed upon separately. [RT I 2008, 19, 132 - entry into force 23.05.2008] (5) In cases of urgency, a request for assistance in criminal offences listed in subsection 491 (2) of this Code may be submitted to a Member State of the European Union through Eurojust. [RT I 2008, 19, 132 - entry into force 23.05.2008] (6) In cases of urgency, Eurojust's National Member for Estonia may prepare a request for assistance in a criminal offence the proceeding of which is to be conducted in Estonia and submit it to a foreign state. [RT I 2008, 19, 132 - entry into force 23.05.2008] (7) The following are competent to submit a request for assistance to foreign states: 1) in pre-trial proceedings, the prosecutor conducting the proceedings; 2) in matters which are subject to court proceedings, the court. [RT I 2008, 19, 132 - entry into force 23.05.2008]
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**§ 464.** Submission of requests for assistance to foreign states (1) Unless otherwise prescribed by an international agreement entered into by the Republic of Estonia, a request for assistance shall be submitted to the Public Prosecutor's Office which shall verify whether the request meets the requirements. The Public Prosecutor's Office shall forward requests in compliance with the requirements to the Ministry of Justice. (2) The Ministry of Justice shall immediately make a decision on the submission of or refusal to submit a request to a foreign state and notify the judicial authority which submitted the request of such decision. Refusal to submit a request shall be reasoned. (3) In cases of urgency, a request may be submitted also through the International Criminal Police Organisation (Interpol) and communicated concurrently through the judicial authorities specified in subsection (1) of this section. The central authority responsible for the national section of the Schengen Information System has the right to add a notice in the Schengen Information System before preparing a request for assistance in order to ensure application of a measure necessary for compliance with the request for assistance. [RT I, 23.02.2011, 1 - entry into force 01.09.2011] (4) If the protection of a witness is requested, the measures of protection shall be agreed upon separately. [RT I 2008, 19, 132 - entry into force 23.05.2008] (5) In cases of urgency, a request for assistance in criminal offences listed in subsection 491 (2) of this Code may be submitted to a Member State of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	European Union through Eurojust. [RT I 2008, 19, 132 - entry into force 23.05.2008] (6) In cases of urgency, Eurojust's National Member for Estonia may prepare a request for assistance in a criminal offence the proceeding of which is to be conducted in Estonia and submit it to a foreign state. [RT I 2008, 19, 132 - entry into force 23.05.2008] (7) The following are competent to submit a request for assistance to foreign states: 1) in pre-trial proceedings, the prosecutor conducting the proceedings; 2) in matters which are subject to court proceedings, the court. [RT I 2008, 19, 132 - entry into force 23.05.2008]
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time 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.	**§ 462. Proceedings conducted by Ministry of Justice and Public Prosecutor's Office concerning requests for assistance received from foreign states** (1) The Ministry of Justice shall verify whether a request for assistance received from a foreign state meets the requirements. A request in compliance with the requirements shall be immediately sent to the Public Prosecutor's Office. (2) The Public Prosecutor's Office shall verify whether compliance with the request is admissible and possible and forward the request to the competent judicial authority for execution. (21) In cases of urgency, a request submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may complied with the consent of the Public Prosecutor's Office before

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the request for assistance is received by the Ministry of Justice. [RT I, 23.02.2011, 1 - entry into force 01.09.2011] (3) The Ministry of Justice shall forward a request for the service of a summons to the court of first instance of the residence or seat of the person for execution. (4) If a request for assistance is submitted through Eurojust, Eurojust's National Member for Estonia shall verify whether the request for assistance meets the requirements and whether compliance with the request for assistance is admissible and possible and forward the request to the Estonian competent judicial authority for execution. [RT I 2008, 19, 132 - entry into force 23.05.2008] **§ 463. Compliance with requests for assistance received from foreign states** (1) Requests for assistance are complied with pursuant to this Code. At the request of a foreign state, a request may be complied with pursuant to procedural provisions different from the provisions of this Code unless this is contrary to the principles of Estonian law. (11) If summoning of a person to court is required for compliance with a request for assistance, service of the summons shall be organised by the court. [RT I 2008, 32, 198 - entry into force 15.07.2008] (2) The materials received as a result of compliance with a request shall be sent to the Ministry of Justice through the Public Prosecutor's Office and the Ministry of Justice shall forward the materials to the requesting state. (3) The materials received as a result of compliance with a request for assistance from a foreign state submitted through Eurojust shall be sent to the requesting state through Eurojust unless otherwise agreed with Eurojust. [RT I 2008, 19, 132 - entry into force 23.05.2008]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	§ 464. Submission of requests for assistance to foreign states (1) Unless otherwise prescribed by an international agreement entered into by the Republic of Estonia, a request for assistance shall be submitted to the Public Prosecutor's Office which shall verify whether the request meets the requirements. The Public Prosecutor's Office shall forward requests in compliance with the requirements to the Ministry of Justice. (2) The Ministry of Justice shall immediately make a decision on the submission of or refusal to submit a request to a foreign state and notify the judicial authority which submitted the request of such decision. Refusal to submit a request shall be reasoned. (3) In cases of urgency, a request may be submitted also through the International Criminal Police Organisation (Interpol) and communicated concurrently through the judicial authorities specified in subsection (1) of this section. The central authority responsible for the national section of the Schengen Information System has the right to add a notice in the Schengen Information System before preparing a request for assistance in order to ensure application of a measure necessary for compliance with the request for assistance. [RT I, 23.02.2011, 1 - entry into force 01.09.2011] (4) If the protection of a witness is requested, the measures of protection shall be agreed upon separately. [RT I 2008, 19, 132 - entry into force 23.05.2008] (5) In cases of urgency, a request for assistance in criminal offences listed in subsection 491 (2) of this Code may be submitted to a Member State of the European Union through Eurojust. [RT I 2008, 19, 132 - entry into force 23.05.2008] (6) In cases of urgency, Eurojust's National Member for Estonia may prepare a request for assistance in a criminal offence the proceeding of which is to be conducted in Estonia and submit it to a foreign state. [RT I 2008, 19, 132 - entry into force 23.05.2008] (7) The following are competent to submit a request for assistance to foreign states: 1) in pre-trial proceedings, the prosecutor conducting the proceedings; 2) in matters which are subject to court proceedings, the court. [RT I 2008, 19, 132 - entry into force 23.05.2008]
Article 34 – Mutual assistance regarding the interception of content data	**§ 462. Proceedings conducted by Ministry of Justice and Public Prosecutor's Office concerning requests for assistance received from**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**foreign states** (1) The Ministry of Justice shall verify whether a request for assistance received from a foreign state meets the requirements. A request in compliance with the requirements shall be immediately sent to the Public Prosecutor's Office. (2) The Public Prosecutor's Office shall verify whether compliance with the request is admissible and possible and forward the request to the competent judicial authority for execution. (21) In cases of urgency, a request submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may complied with the consent of the Public Prosecutor's Office before the request for assistance is received by the Ministry of Justice. [RT I, 23.02.2011, 1 - entry into force 01.09.2011] (3) The Ministry of Justice shall forward a request for the service of a summons to the court of first instance of the residence or seat of the person for execution. (4) If a request for assistance is submitted through Eurojust, Eurojust's National Member for Estonia shall verify whether the request for assistance meets the requirements and whether compliance with the request for assistance is admissible and possible and forward the request to the Estonian competent judicial authority for execution. [RT I 2008, 19, 132 - entry into force 23.05.2008] **§ 463. Compliance with requests for assistance received from foreign states** (1) Requests for assistance are complied with pursuant to this Code. At the request of a foreign state, a request may be complied with pursuant to procedural provisions different from the provisions of this Code unless this is contrary to the principles of Estonian law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(11) If summoning of a person to court is required for compliance with a request for assistance, service of the summons shall be organised by the court. [RT I 2008, 32, 198 - entry into force 15.07.2008] (2) The materials received as a result of compliance with a request shall be sent to the Ministry of Justice through the Public Prosecutor's Office and the Ministry of Justice shall forward the materials to the requesting state. (3) The materials received as a result of compliance with a request for assistance from a foreign state submitted through Eurojust shall be sent to the requesting state through Eurojust unless otherwise agreed with Eurojust. [RT I 2008, 19, 132 - entry into force 23.05.2008] **§ 464.** Submission of requests for assistance to foreign states (1) Unless otherwise prescribed by an international agreement entered into by the Republic of Estonia, a request for assistance shall be submitted to the Public Prosecutor's Office which shall verify whether the request meets the requirements. The Public Prosecutor's Office shall forward requests in compliance with the requirements to the Ministry of Justice. (2) The Ministry of Justice shall immediately make a decision on the submission of or refusal to submit a request to a foreign state and notify the judicial authority which submitted the request of such decision. Refusal to submit a request shall be reasoned. (3) In cases of urgency, a request may be submitted also through the International Criminal Police Organisation (Interpol) and communicated concurrently through the judicial authorities specified in subsection (1) of this section. The central authority responsible for the national section of the Schengen Information System has the right to add a notice in the Schengen Information System before preparing a request for assistance in order to ensure application of a measure necessary for compliance with the request for assistance. [RT I, 23.02.2011, 1 - entry into force 01.09.2011] (4) If the protection of a witness is requested, the measures of protection shall be agreed upon separately. [RT I 2008, 19, 132 - entry into force 23.05.2008] (5) In cases of urgency, a request for assistance in criminal offences listed in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	subsection 491 (2) of this Code may be submitted to a Member State of the European Union through Eurojust. [RT I 2008, 19, 132 - entry into force 23.05.2008] (6) In cases of urgency, Eurojust's National Member for Estonia may prepare a request for assistance in a criminal offence the proceeding of which is to be conducted in Estonia and submit it to a foreign state. [RT I 2008, 19, 132 - entry into force 23.05.2008] (7) The following are competent to submit a request for assistance to foreign states: 1) in pre-trial proceedings, the prosecutor conducting the proceedings; 2) in matters which are subject to court proceedings, the court. [RT I 2008, 19, 132 - entry into force 23.05.2008]
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**Law ratifying the Convention on Cybercrime** **§ 2. Declarations** (3) Pursuant to the Article 35(1) of the Convention the Republic of Estonia appoints Police and Border Guard Board as point of contact.
Article 42 – Reservations	

Back to the Table of Contents

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

Back to the Table of Contents