Latvia

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

[reference to the provisions of the Budapest Convention]

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

State:	
Signature of the Budapest Convention:	05/05/2004
Ratification/accession:	14/02/2007

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 Criminal Law does not provide for any definitions; however, in the Electronic Communications Law, for instance, the following is included: • electronic communications merchant – a merchant or a branch of a foreign merchant who has the right to perform commercial activity, to ensure a public electronic communications network or provide electronic communications services in accordance with the procedures laid down in the Electronic Communications Law; • electronic communications service – a service that is usually ensured for remuneration and which wholly or mainly consists of the transmission of signals in electronic communications networks; • electronic communications service provider – an electronic communications merchant who provides publicly accessible electronic communications services, utilising the public electronic communications network; • electronic communications network – transmission systems, switching and routing equipment (including network elements which are not being used) and other resources, which irrespective of the type of transmitted

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	information permits the transmission of signals utilising wires, radio waves, optical or other electromagnetic means in networks, including: a) satellite networks, fixed networks (channel and packet switching networks, including Internet) and mobile terrestrial electronic communications networks, b) networks, which are utilised for radio and television signal distribution, c) cable television and cable radio networks, electricity cables systems to the extent that they are utilised in order to transmit signals; • terminal equipment – equipment (for example, telephone sets, facsimile machines, modems, data transmission equipment, private automatic telephone exchanges, private networks, and public pay telephones) that is intended for direct or indirect connection to public electronic communications network termination points; traffic data – any information or data, which is processed in order to transmit information by an electronic communications network or to prepare accounts and register payments, except the content of transmitted information.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	According to provisions of the Criminal Law, the following acts are criminalized: 1) violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (namely, illegal interception; Article 144):

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for a person who commits intentional violation of the confidentiality of personal correspondence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 1); for a person who commits unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a telecommunications network in which such data is present, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 2); for committing the acts provided for in paragraph one or two, if such are committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 3); 2) obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment (Article 193^1): for a person who commits obtaining or distribution of such data as enable illegal utilisation of financial instruments or means of payment, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 193^1 paragraph 1); for a person who commits utilisation of such data as enable illegal utilisation of financial instruments or means of payment, or who commits manufacture or adaptation of software or equipment for the commission of the crimes provided for by Article 193 of this Law, or commits obtaining, storage or distribution of such software or equipment for the same purpose, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 193^1 paragraph 2); for a person who commits the acts provided for by paragraph one or two, if commission thereof is in an organised group, the applicable punishment is

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	deprivation of liberty for a term of two years and up to ten years, with or without confiscation of property and with police supervision for a term up to three years (Article 1931 paragraph 3). 3) arbitrary accessing automated data processing systems (Article 241): for a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 241 paragraph 1); for the criminal offence provided for in paragraph one, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 2); for the acts provided for in paragraph one, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 3); 4) interference in the operation of automated data processing systems and illegal actions with the information included in such systems (Article 243): for a person who commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby, the applicable punishment is deprivation of liberty for a term up to two years or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 1); for a person who commits knowingly interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 2); for the criminal offence provided for in paragraph one or two, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with or without police supervision for a term up to three years (Article 243 paragraph 3); for the acts provided for in paragraph one or two, if they have been committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to seven years, with or without confiscation of property and with or without probationary supervision for a term up to three years (Article 243 paragraph 5); 5) illegal operations with automated data processing system resource influencing devices (Article 244): for a person who commits the illegal manufacture, adaptation for utilisation, sale, distribution or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for purposes of committing a criminal offence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 1);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for a person who commits the same acts, if serious consequences has been caused thereby, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 2); 6) acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244[1]): for a person who commits electronic communications network terminal equipment identification in an electronic communications network for necessary data alterations or the acquisition, storage or distribution of data intended for such purposes, as well as the acquisition, development, storage or distribution of programs or equipment intended for such purposes without the consent of the manufacturer or the authorised person thereof, if such activities have been committed for purposes of acquiring property or if it has been committed by a group of persons pursuant to prior agreement, or if it has caused significant harm, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine. 7) article 245 (violation of safety provisions regarding information systems): for a person who commits violation of provisions regarding information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions, if such has been a cause of stealing, destruction or damage of the information, or other substantial harm has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine.
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 internationally, 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	According to provisions of the Criminal Law, the following acts are criminalized: 1) violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (namely, illegal interception; Article 144): for a person who commits intentional violation of the confidentiality of personal correspondence, the applicable punishment is deprivation of liberty for

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 1); for a person who commits unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a telecommunications network in which such data is present, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 2); for committing the acts provided for in paragraph one or two, if such are committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 3); 2) obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment (Article 193[1]): for a person who commits obtaining or distribution of such data as enable illegal utilisation of financial instruments or means of payment, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 193[1] paragraph 1); for a person who commits utilisation of such data as enable illegal utilisation of financial instruments or means of payment, or who commits manufacture or adaptation of software or equipment for the commission of the crimes provided for by Article 193 of this Law, or commits obtaining, storage or distribution of such software or equipment for the same purpose, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 193[1] paragraph 2); for a person who commits the acts provided for by paragraph one or two, if commission thereof is in an organised group, the applicable punishment is

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	deprivation of liberty for a term of two years and up to ten years, with or without confiscation of property and with police supervision for a term up to three years (Article 1931 paragraph 3). 3) arbitrary accessing automated data processing systems (Article 241): for a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 241 paragraph 1); for the criminal offence provided for in paragraph one, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 2); for the acts provided for in paragraph one, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 3); 4) interference in the operation of automated data processing systems and illegal actions with the information included in such systems (Article 243): for a person who commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 243

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	paragraph 1); for a person who commits knowingly interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 2); for the criminal offence provided for in paragraph one or two, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with or without police supervision for a term up to three years (Article 243 paragraph 3); for the acts provided for in paragraph one or two, if they have been committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to seven years, with or without confiscation of property and with or without probationary supervision for a term up to three years (Article 243 paragraph 5); 5) illegal operations with automated data processing system resource influencing devices (Article 244): for a person who commits the illegal manufacture, adaptation for utilisation, sale, distribution or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for purposes of committing a criminal offence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 1);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for a person who commits the same acts, if serious consequences has been caused thereby, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 2); 6) acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244[1]): for a person who commits electronic communications network terminal equipment identification in an electronic communications network for necessary data alterations or the acquisition, storage or distribution of data intended for such purposes, as well as the acquisition, development, storage or distribution of programs or equipment intended for such purposes without the consent of the manufacturer or the authorised person thereof, if such activities have been committed for purposes of acquiring property or if it has been committed by a group of persons pursuant to prior agreement, or if it has caused significant harm, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine. 7) article 245 (violation of safety provisions regarding information systems): for a person who commits violation of provisions regarding information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions, if such has been a cause of stealing, destruction or damage of the information, or other substantial harm has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	According to provisions of the Criminal Law, the following acts are criminalized: 1) violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (namely, illegal interception; Article 144): for a person who commits intentional violation of the confidentiality of personal correspondence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 1); for a person who commits unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a telecommunications network in which such data is present, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 2); for committing the acts provided for in paragraph one or two, if such are committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 3); 2) obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment (Article 193^1): for a person who commits obtaining or distribution of such data as enable illegal utilisation of financial instruments or means of payment, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 193^1 paragraph 1); for a person who commits utilisation of such data as enable illegal utilisation of financial instruments or means of payment, or who commits manufacture or adaptation of software or equipment for the commission of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	crimes provided for by Article 193 of this Law, or commits obtaining, storage or distribution of such software or equipment for the same purpose, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 193[1] paragraph 2); for a person who commits the acts provided for by paragraph one or two, if commission thereof is in an organised group, the applicable punishment is deprivation of liberty for a term of two years and up to ten years, with or without confiscation of property and with police supervision for a term up to three years (Article 1931 paragraph 3). 3) arbitrary accessing automated data processing systems (Article 241): for a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 241 paragraph 1); for the criminal offence provided for in paragraph one, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 2); for the acts provided for in paragraph one, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 3); 4) interference in the operation of automated data processing systems and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	illegal actions with the information included in such systems (Article 243): for a person who commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 1); for a person who commits knowingly interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 2); for the criminal offence provided for in paragraph one or two, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with or without police supervision for a term up to three years (Article 243 paragraph 3); for the acts provided for in paragraph one or two, if they have been committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to seven years, with or without confiscation of property and with or without probationary supervision for a term up to three years (Article 243 paragraph 5); 5) illegal operations with automated data processing system resource influencing devices (Article 244): for a person who commits the illegal manufacture, adaptation for

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	utilisation, sale, distribution or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for purposes of committing a criminal offence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 1); for a person who commits the same acts, if serious consequences has been caused thereby, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 2); 6) acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244[1]): for a person who commits electronic communications network terminal equipment identification in an electronic communications network for necessary data alterations or the acquisition, storage or distribution of data intended for such purposes, as well as the acquisition, development, storage or distribution of programs or equipment intended for such purposes without the consent of the manufacturer or the authorised person thereof, if such activities have been committed for purposes of acquiring property or if it has been committed by a group of persons pursuant to prior agreement, or if it has caused significant harm, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine. 7) article 245 (violation of safety provisions regarding information systems): for a person who commits violation of provisions regarding information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions, if such has been a cause of stealing, destruction or damage of the information, or other substantial harm

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine.
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	According to provisions of the Criminal Law, the following acts are criminalized: 1) violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (namely, illegal interception; Article 144): for a person who commits intentional violation of the confidentiality of personal correspondence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 1); for a person who commits unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a telecommunications network in which such data is present, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 2); for committing the acts provided for in paragraph one or two, if such are committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 3); 3) arbitrary accessing automated data processing systems (Article 241): for a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 241 paragraph 1); for the criminal offence provided for in paragraph one, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 2); for the acts provided for in paragraph one, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 3); 4) interference in the operation of automated data processing systems and illegal actions with the information included in such systems (Article 243): for a person who commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 1); for a person who commits knowingly interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 2);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for the criminal offence provided for in paragraph one or two, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with or without police supervision for a term up to three years (Article 243 paragraph 3); for the acts provided for in paragraph one or two, if they have been committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to seven years, with or without confiscation of property and with or without probationary supervision for a term up to three years (Article 243 paragraph 5); 5) illegal operations with automated data processing system resource influencing devices (Article 244): for a person who commits the illegal manufacture, adaptation for utilisation, sale, distribution or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for purposes of committing a criminal offence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 1); for a person who commits the same acts, if serious consequences has been caused thereby, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 2); 6) acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244[1]):

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for a person who commits electronic communications network terminal equipment identification in an electronic communications network for necessary data alterations or the acquisition, storage or distribution of data intended for such purposes, as well as the acquisition, development, storage or distribution of programs or equipment intended for such purposes without the consent of the manufacturer or the authorised person thereof, if such activities have been committed for purposes of acquiring property or if it has been committed by a group of persons pursuant to prior agreement, or if it has caused significant harm, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine. 7) article 245 (violation of safety provisions regarding information systems): for a person who commits violation of provisions regarding information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions, if such has been a cause of stealing, destruction or damage of the information, or other substantial harm has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and	According to provisions of the Criminal Law, the following acts are criminalized: 1) violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (namely, illegal interception; Article 144): for a person who commits intentional violation of the confidentiality of personal correspondence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 1); for a person who commits unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	telecommunications network in which such data is present, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 2); for committing the acts provided for in paragraph one or two, if such are committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 3); 2) 3) arbitrary accessing automated data processing systems (Article 241): for a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 241 paragraph 1); for the criminal offence provided for in paragraph one, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 2); for the acts provided for in paragraph one, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 3); 4) interference in the operation of automated data processing systems and illegal actions with the information included in such systems (Article 243):

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for a person who commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 1); for a person who commits knowingly interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 2); for the criminal offence provided for in paragraph one or two, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with or without police supervision for a term up to three years (Article 243 paragraph 3); for the acts provided for in paragraph one or two, if they have been committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to seven years, with or without confiscation of property and with or without probationary supervision for a term up to three years (Article 243 paragraph 5); 5) illegal operations with automated data processing system resource influencing devices (Article 244): for a person who commits the illegal manufacture, adaptation for utilisation, sale, distribution or storage of such tool (device, software, computer

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for purposes of committing a criminal offence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 1); for a person who commits the same acts, if serious consequences has been caused thereby, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 2); 6) acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244[1]): for a person who commits electronic communications network terminal equipment identification in an electronic communications network for necessary data alterations or the acquisition, storage or distribution of data intended for such purposes, as well as the acquisition, development, storage or distribution of programs or equipment intended for such purposes without the consent of the manufacturer or the authorised person thereof, if such activities have been committed for purposes of acquiring property or if it has been committed by a group of persons pursuant to prior agreement, or if it has caused significant harm, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine. 7) article 245 (violation of safety provisions regarding information systems): for a person who commits violation of provisions regarding information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions, if such has been a cause of stealing, destruction or damage of the information, or other substantial harm

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine.
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.	The following acts have been criminalized: 1) illegal activities involving personal data of natural persons (Article 145): for illegal activities involving personal data of a natural person, if it has caused substantial harm, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 1); for illegal activities involving personal data of a natural person, if they have been performed by a personal data processing administrator or operator for the purpose of vengeance, acquisition of property or blackmail, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 2); for influencing a personal data processing administrator or operator or the data subject, using violence or threats or using trust in bad faith, or using deceit in order to perform illegal activities involving personal data of a natural person, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 3); 2) fraud in an automated data processing system (Article 177^1): for a person who commits the knowingly entering of false data into an automated data processing system for the acquisition of the property of another person or the rights to such property, or the acquisition of other material benefits, in order to influence the operation of the resources thereof (computer fraud), the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 177^1 paragraph 1); for a person who commits computer fraud, if it has been committed by a group of persons pursuant to prior agreement, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 177^1 paragraph 2);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for a person who commits computer fraud, if it has been committed on a large scale or if it has been committed in an organised group, the applicable punishment is deprivation of liberty for a term of two years and up to ten years, or a fine, with or without confiscation of property and with or without police supervision for a term up to three years (Article 177[1] paragraph 3). As regards spam, it shall be noted that according to Article 20416 of the Latvian Administrative Violations Code (on violation of the prohibition on sending commercial information) in the case of violation of the prohibition on sending commercial information as specified in the law, a warning shall be issued or a fine shall be imposed on natural persons in an amount from 140 to 500 euros, but for legal persons – from 700 to 7100 euros.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	The following acts have been criminalized: 1) illegal activities involving personal data of natural persons (Article 145): for illegal activities involving personal data of a natural person, if it has caused substantial harm, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 1); for illegal activities involving personal data of a natural person, if they have been performed by a personal data processing administrator or operator for the purpose of vengeance, acquisition of property or blackmail, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 2); for influencing a personal data processing administrator or operator or the data subject, using violence or threats or using trust in bad faith, or using deceit in order to perform illegal activities involving personal data of a natural person, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 3); 2) fraud in an automated data processing system (Article 177[1]): for a person who commits the knowingly entering of false data into an automated data processing system for the acquisition of the property of another person or the rights to such property, or the acquisition of other material benefits, in order to influence the operation of the resources thereof (computer fraud), the applicable punishment is deprivation of liberty for a term up to three

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	years or temporary deprivation of liberty, or community service, or a fine (Article 177[1] paragraph 1); for a person who commits computer fraud, if it has been committed by a group of persons pursuant to prior agreement, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 177[1] paragraph 2); for a person who commits computer fraud, if it has been committed on a large scale or if it has been committed in an organised group, the applicable punishment is deprivation of liberty for a term of two years and up to ten years, or a fine, with or without confiscation of property and with or without police supervision for a term up to three years (Article 177[1] paragraph 3). 3) arbitrary accessing automated data processing systems (Article 241): for a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 241 paragraph 1); for the criminal offence provided for in paragraph one, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 2); for the acts provided for in paragraph one, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 3); 4) interference in the operation of automated data processing systems and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	illegal actions with the information included in such systems (Article 243): for a person who commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 1); for a person who commits knowingly interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 2); for the criminal offence provided for in paragraph one or two, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with or without police supervision for a term up to three years (Article 243 paragraph 3); for the acts provided for in paragraph one or two, if they have been committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to seven years, with or without confiscation of property and with or without probationary supervision for a term up to three years (Article 243 paragraph 5); As regards spam, it shall be noted that according to Article 204.[16] of the Latvian Administrative Violations Code (on violation of the prohibition on sending commercial information) in the case of violation of the prohibition on sending commercial information as specified in the law, a warning shall be issued or a

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	fine shall be imposed on natural persons in an amount from 140 to 500 euros, but for legal persons – from 700 to 7100 euros.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-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.	The following acts are criminalized: 1) encouraging to involve in sexual acts (Article 162[1]): for a person who encourages person who has not attained the age of sixteen years to involve in sexual acts or encourages such person to meet with the aim to commit sexual acts or enter into a sexual relationship using information or communication technologies or other means of communication, if such act has been committed by a person who has attained the age of majority, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine and with probationary supervision for a term up to five years; for the acts provided for in paragraph one, if it has been committed against an under aged person, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with probationary supervision for a term up to five years; 2) violation of provisions regarding the demonstration of a pornographic performance, restriction of entertainment of intimate nature and handling of a material of pornographic nature (Article 166): for a person who commits the visiting or demonstration of such pornographic performance or the handling of such materials of pornographic nature which contain child pornography, sexual activities of people with animals, necrophilia or sexual gratification in a violent way, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property and with probationary supervision for a term up to three years (Article 166 paragraph 2); for a person who commits encouraging, involvement, forced participation or utilisation of minors in a pornographic performance or the production of a material of pornographic nature, the applicable punishment is deprivation of liberty for a term up to six years, with or without confiscation of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	property and with probationary supervision for a term up to three years (Article 166 paragraph 3); for a person who commits encouraging, involvement, forced participation or utilisation of persons who have not attained the age of sixteen years in a pornographic performance or the production of a material of pornographic nature, the applicable punishment is deprivation of liberty for a term of three years and up to twelve years, with or without confiscation of property and with probationary supervision for a term up to three years (Article 166 paragraph 4); for a person who commits the acts provided for in paragraph three or four, if they have been committed by an organised group or if they have been committed by means of violence, the applicable punishment is deprivation of liberty for a term of five years and up to fifteen years, with or without confiscation of property and with probationary supervision for a term up to three years (Article 166 paragraph 5). Latvia has fully transposed into national law Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. The transposition has been completed by the Amendments in Criminal Law (Section 48, 159-162[1], 164-166).
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting	Article 148 (infringement of copyright and neighboring rights): for a person who commits infringement of copyright or neighboring right, if such infringement has caused substantial harm to rights and interests protected by law of a person, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 148 paragraph 1); for a person who commits the criminal offence provided for in paragraph one of this Article, if it has been committed by a group of persons pursuant to prior agreement, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine (Article 148 paragraph 2); for a person who commits infringement of copyright or neighboring right if it is committed in large scale or by an organized group, or by compelling, by

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	means of violence, threats or blackmail, the renouncing of authorship, or commits compelling of joint authorship, if it is committed by means of violence, threats or blackmail, the applicable punishment is deprivation of liberty for a term up to six years, with deprivation of the right to engage in specific employment for a term up to five years and with or without police supervision for a term up to three years (Article 148 paragraph 3).
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.	According to the Criminal Law Article 18 (Participation of Several Persons in a Criminal Offence) The participation by two or several persons knowingly in joint commission of an intentional criminal offence is participation or joint participation. Article 19. Participation Criminal acts committed knowingly by which two or several persons (that is, a group) jointly, knowing such, have directly committed an intentional criminal offence shall be considered to be participation (joint commission). Each of such persons is a participant (joint perpetrator) in the criminal offence. Article 20. Joint Participation (1) An act or failure to act committed knowingly by which a person (joint participant) has jointly with another person (perpetrator) participated in the commission of an intentional criminal offence, but he himself or she herself has not been the direct perpetrator of it, shall be considered to be joint participation. Organisers, instigators, and abettors are joint participants in a criminal offence. (2) A person who has organised or directed the commission of a criminal offence shall be considered to be an organiser.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) A person who has encouraged another person to commit a criminal offence shall be considered to be an instigator. (4) A person who has knowingly promoted the commission of a criminal offence, providing advice, direction, or means, or removing impediments for the commission of such, as well as a person who has previously promised to conceal the perpetrator or joint participant, the instrumentalities or means for committing the criminal offence, trail of the criminal offence or the objects acquired by criminal means or has previously promised to acquire or to dispose these objects, shall be considered to be an abettor. (5) A joint participant shall be held liable in accordance with the same Section of this Law which provides for the liability of the perpetrator. (6) Individual constituent elements of a criminal offence which refer to a perpetrator or joint participant do not affect the liability of other participants or joint participants. (7) If a joint participant has not had the knowledge of a criminal offence committed by a perpetrator or other joint participants, he or she shall not be held criminally liable for such. (8) If the perpetrator has not completed the offence for reasons independent of his or her will, the joint participants are liable for joint participation in the relevant attempted offence. If the perpetrator has not commenced commission of the offence, the joint participants are liable for preparation for the relevant offence. (9) Voluntary withdrawal, by an organiser or instigator from completing of commission of a criminal offence shall be considered as such only in cases when he or she, in due time, has done everything possible to prevent the commission with his or her joint participation of the contemplated criminal offence and this offence has not been committed. An abettor shall not be held criminally liable if he or she has voluntarily refused to provide the promised assistance before commencement of the criminal offence. Article 21. Organised Groups

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) An organised group is an association formed by more than two persons which has been created for the purpose of jointly committing one or several crimes and the participants of which in accordance with previous agreement have divided responsibilities. (2) Liability of a person for the commission of an offence within an organised group shall apply in the cases set out in this Law for formation and leadership of a group, and for participation in preparation for a serious or especially serious crime or in commission of a crime, irrespective of the role of the person in the jointly committed offence. Article 22. Concealing without a Prior Promise and Failure to Inform (1) Concealment without a prior promise of a perpetrator or a joint participant in a crime, as well as of instrumentalities or means for committing a crime or trail of a crime, and failure to inform regarding a crime are not joint participation, and criminal liability for such shall apply only in the cases provided for in this Law. (2) The betrothed, spouse, parents, children, brothers and sisters, grandparents and grandchildren of a person who has committed a crime, as well as the person with whom the natural person who has committed a crime is living together and with whom he or she has a joint (single) household are not liable for concealment without a prior promise or failure to inform. (3) In the cases set out in this Law other persons are also not liable for failure to inform. Article 23. Separate (Unitary) Criminal Offence (1) A separate (unitary) criminal offence is one offence (act or failure to act) which has the constituent elements of one criminal offence, or also two or several mutually related criminal offences encompassed by the unitary purpose of the offender and which correspond to the constituent elements of only one criminal offence. (2) A separate (unitary) criminal offence is also constituted by continuous and continuing criminal offences.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) A separate continuous criminal offence is constituted by several mutually related similar criminal acts which are directed to a common objective if they are encompassed by the unitary purpose of the offender, and therefore in their totality they form one criminal offence. (4) A separate continuing criminal offence is the uninterrupted realisation of the elements of one criminal offence (act or failure to act) which is related to consequent continuing non-fulfilment of obligations which has been imposed upon the offender by the law with threat of criminal prosecution. Article 7. Classification of Criminal Offences (1) Criminal offences shall be divided into criminal violations and crimes according to the nature and harm of the threat to the interests of a person or the society. Crimes shall be divided as follows: less serious crimes, serious crimes and especially serious crimes. (2) A criminal violation is an offence for which the deprivation of liberty for a period exceeding fifteen days, but not exceeding three months (temporary deprivation of liberty), or a type of lesser punishment is provided for in this Law. (3) A less serious crime is an intentional offence for which the deprivation of liberty for a period exceeding three months but not exceeding three years is provided for in this Law, as well as an offence which has been committed through negligence and for which the deprivation of liberty for a period not exceeding eight years is provided for in this Law. (4) A serious crime is an intentional offence for which the deprivation of liberty for a period exceeding three years but not exceeding eight years is provided for in this Law, as well as an offence which has been committed through negligence and for which the deprivation of liberty for a time period exceeding eight years is provided for in this Law. (5) An especially serious crime is an intentional offence for which the deprivation of liberty for a period exceeding eight years or life imprisonment is provided for in this Law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) If this Law provides for the deprivation of liberty for a period not exceeding five years for a crime, also a type of lesser punishment may be provided for therein for the relevant crime.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a 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.	**Section 70.[1] Basis for the Application of a Coercive Measure to a Legal Person** For the criminal offences provided for in the Special Part of this Law, a court or in the cases provided for by the Law - a public prosecutor may apply a coercive measure to a legal person governed by private law, including State or local government capital company, as well as partnership, if a natural person has committed the offence in the interests of the legal person, for the benefit of the person or as a result of insufficient supervision or control, acting individually or as a member of the collegial authority of the relevant legal person: 1) on the basis of the right to represent the legal person or act on the behalf thereof; 2) on the basis of the right to take a decision on behalf of the legal person; 3) in implementing control within the scope of the legal person. [*14 March 2013]*
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. Application of The Criminal Law in the Territory of Latvia** (1) The liability of a person who has committed a criminal offence in the territory of Latvia shall be determined in accordance with this Law. (2) If a foreign diplomatic representative, or other person who, in accordance with the laws in force or international agreements binding upon the Republic of Latvia, is not subject to the jurisdiction of the Republic of Latvia, has committed a criminal offence in the territory of Latvia, the issue of this person being held

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	criminally liable shall be decided by diplomatic procedures or in accordance with a mutual agreement of the states. **Section 4. Applicability of The Criminal Law Outside the Territory of Latvia** (1) Latvian citizens, non-citizens, and foreigners who have a permanent residence permit in the Republic of Latvia, shall be held liable, in accordance with this Law, in the territory of Latvia for an offence committed in the territory of another state or outside the territory of any state irrespective of whether it has been recognised as criminal and punishable in the territory of commitment. (1^1) For an offence committed by a natural person acting in the interests of a legal person registered in the Republic of Latvia, for the benefit of the person or as a result of insufficient supervision or control thereof in the territory of another state or outside the territory of any state irrespective of whether it has been recognised as criminal and punishable in the territory of commitment the legal person may be applied the coercive measures provided for in this Law. (2) Soldiers of the Republic of Latvia who are located outside the territory of Latvia shall be held liable for criminal offences in accordance with this Law, unless it is otherwise provided for in international agreements binding upon the Republic of Latvia. (3) Foreigners who do not have permanent residence permits in the Republic of Latvia and who have committed serious or especially serious crimes in the territory of another state which have been directed against the Republic of Latvia or against the interests of its inhabitants, shall be held criminally liable in accordance with this Law irrespective of the laws of the state in which the crime has been committed, if they have not been held criminally liable or committed to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	stand trial in accordance with the laws of the state where the crime was committed. (4) Foreigners who do not have a permanent residence permit in the Republic of Latvia and who have committed a criminal offence in the territory of another state or outside the territory of any state, in the cases provided for in international agreements binding upon the Republic of Latvia, irrespective of the laws of the state in which the offence has been committed, shall be held liable in accordance with this Law, if they have not been held criminally liable for such offence or committed to stand trial in the territory of another state. *[17 October 2002; 16 December 2004; 21 May 2009; 21 October 2010; 25 September 2014]* **Section 5. Time when The Criminal Law is In Force** (1) The criminality and punishability of an offence (act or failure to act) are determined by the law which was in force at the time of committing the offence. (2) A law which recognises an offence as not punishable, reduces the punishment or is otherwise beneficial to a person, unless otherwise provided for in the applicable law, has retrospective effect, that is, it applies to offences which have been committed prior to the applicable law coming into force, as well as to a person who is serving a punishment or has served a punishment but regarding whom conviction remains in effect. (3) A law which recognises an offence as punishable, increases the punishment, or is otherwise not beneficial to a person, does not have retrospective effect.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 6. Concept of a Criminal Offence (1) A harmful offence (act or failure to act) committed deliberately (intentionally) or through negligence, provided for in this Law, and for the commission of which criminal punishment is set out shall be considered a criminal offence. (2) An offence (act or failure to act) which has the constituent elements of an offence set out in this Law, but has been committed in circumstances which exclude criminal liability, shall not be considered criminal. *[13 December 2012; 1 April 2013]* **Section 7. Classification of Criminal Offences** (1) Criminal offences shall be divided into criminal violations and crimes according to the nature and harm of the threat to the interests of a person or the society. Crimes shall be divided as follows: less serious crimes, serious crimes and especially serious crimes. (2) A criminal violation is an offence for which the deprivation of liberty for a period exceeding fifteen days, but not exceeding three months (temporary deprivation of liberty), or a type of lesser punishment is provided for in this Law. (3) A less serious crime is an intentional offence for which the deprivation of liberty for a period exceeding three months but not exceeding three years is provided for in this Law, as well as an offence which has been committed through negligence and for which the deprivation of liberty for a period not exceeding eight years is provided for in this Law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) A serious crime is an intentional offence for which the deprivation of liberty for a period exceeding three years but not exceeding eight years is provided for in this Law, as well as an offence which has been committed through negligence and for which the deprivation of liberty for a time period exceeding eight years is provided for in this Law. (5) An especially serious crime is an intentional offence for which the deprivation of liberty for a period exceeding eight years or life imprisonment is provided for in this Law. (6) If this Law provides for the deprivation of liberty for a period not exceeding five years for a crime, also a type of lesser punishment may be provided for therein for the relevant crime. *[21 May 2009; 1 December 2011; 13 December 2012]* **Section 8. Forms of Guilt** (1) Only a person who has committed a criminal offence deliberately (intentionally) or through negligence may be found guilty of it. (2) When determining the form of guilt of the person who has committed a criminal offence the mental state of the person in relation to the objective elements of the criminal offence must be established. **Section 9. Commission of a Criminal Offence Deliberately (Intentionally)** (1) A criminal offence shall be considered to have been committed deliberately (intentionally) if the person has committed it with a direct or indirect intent.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) A criminal offence shall be considered to have been committed with a direct intent if the person has been aware of the harm caused by his or her act or failure to act and has knowingly committed or allowed it or also been aware of the harm caused by his or her act or failure to act, foreseen the harmful consequences of the offence and has desired them. (3) A criminal offence shall be considered to have been committed with an indirect intent if the person has been aware of the harm caused by his or her act or failure to act, foreseen the harmful consequences of the offence and, although has not desired such consequences, has knowingly allowed them to result. [*13 December 2012]* **Section 10. Commission of a Criminal Offence through Negligence** (1) A criminal offence shall be considered to be committed through negligence if the person has committed it through criminal self-reliance or criminal neglect. (2) A criminal offence shall be considered to have been committed through criminal self-reliance if the person has foreseen the possibility that the harmful consequences of his or her act or failure to act would result and nevertheless carelessly relied on these being prevented. (3) A criminal offence shall be considered to have been committed through criminal neglect if the person did not foresee the possibility that the consequences of his or her act or failure to act would result, although according to the actual circumstances of the offence he or she should have and could have foreseen the referred to harmful consequences.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) An offence provided for in this Law shall not be criminally punishable if the person did not foresee and should not and could not have foreseen the possibility that harmful consequences of his or her act or failure to act would result. [*13 December 2012]* **Section 11. Age at which the Criminal Liability Applies** A natural person who, on the day of the commission of a criminal offence, has attained fourteen years of age may be held criminally liable. An underaged person, that is, a person who has not attained fourteen years of age, may not be held criminally liable. Section 47. Mitigating Circumstances (1) The following circumstances shall be considered as circumstances mitigating the liability: 1) the perpetrator of the criminal offence has admitted his or her guilt, has freely confessed and has regretted the criminal offence committed; 2) the offender has actively furthered the disclosure and investigation of the criminal offence; 3) the offender has voluntarily compensated the harm caused by the criminal offence to the victim or has eliminated the harm caused; 4) the offender has facilitated the disclosure of a crime of another person; 5) the criminal offence was committed as a result of unlawful or immoral behaviour of the victim;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	6) the criminal offence was committed exceeding the conditions regarding the necessary self-defence, extreme necessity, detention of the person committing the criminal offence, justifiable professional risk, the legality of the execution of a command and order; 7) the criminal offence was committed by a person in a state of diminished mental capacity. (2) In determining a punishment, circumstances which are not provided for in this Law and which are related to the criminal offence committed, may be considered as circumstances mitigating the liability. (3) A circumstance, which is provided for in this Law as a constituent element of a criminal offence, may not be considered to be a mitigating circumstance. **Section 48. Aggravating Circumstances** (1) The following may be considered to be aggravating circumstances: 1) the criminal offence constitutes recidivism of criminal offences; 2) the criminal offence was committed while in a group of persons; 3) the criminal offence was committed, taking advantage in bad faith of an official position or trust of another person; 4) the criminal offence has caused serious consequences; 5) the criminal offence was committed against a woman, knowing her to be pregnant;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	6) the criminal offence was committed against a person who has not attained eighteen years of age or against a person by taking advantage of his or her condition of helplessness or of infirmity due to old-age; 7) the criminal offence was committed against a person taking advantage of his or her official, financial or other dependence on the offender; 8) the criminal offence was committed with particular cruelty or with humiliation of the victim; 9) the criminal offence was committed by taking advantage of the circumstances of a public disaster or during an emergency situation or a state of exception; 10) the criminal offence was committed employing weapons or explosives, or in some other generally dangerous way; 11) the criminal offence was committed out of a desire to acquire property; 12) the criminal offence was committed under the influence of alcohol, narcotic, psychotropic, toxic or other intoxicating substances; 13) the person committing the criminal offence, for the purpose of having his or her punishment reduced, has knowingly provided false information regarding a criminal offence committed by another person; 14) the criminal offence was committed due to racist, national, ethnic or religious motives; 15) the criminal offence related to violence or threats of violence, or the criminal offence against morality and sexual inviolability was committed against

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a person to whom the perpetrator of a criminal offence is related in the first or second degree of kinship, or against the spouse or former spouse, or against a person with whom the perpetrator of a criminal offence is or has been in continuous intimate relationships, or against a person with whom the perpetrator of a criminal offence has a joint (single) household; 16) the criminal offence related to violence or threats of violence, or an intentional criminal offence against health or morality and sexual inviolability of a person was committed at the presence of a minor. (2) Taking into account the nature of the criminal offence, it may be decided not to consider any of the circumstances referred to in Paragraph one of this Section as aggravating. (3) In determining punishment, such circumstances may not be considered as aggravating which are not set out in this Law. (4) A circumstance which is provided for in this Law as a constituent element of a criminal offence shall not be considered an aggravating circumstance. *[27 May 2004; 12 October 2006; 21 October 2010; 13 December 2012; 15 May 2014; 25 September 2014; 8 June 2017]* **Section 70.^{2} Types of Coercive Measures Applicable to a Legal Person** (1) For a legal person one of the following coercive measures may be specified: 1) liquidation; 2) restriction of rights; 3) confiscation of property; 4) recovery of money.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) For a legal person one or several of the coercive measures provided for in Paragraph one of this Section may be applied. In applying liquidation, other coercive measures shall not be specified. (3) The procedures for executing coercive measures shall be determined in accordance with the law. (4) For a criminal violation, a less serious crime or a serious crime for which deprivation of liberty for a period of up to five years is provided for in the Special Part of this Law a public prosecutor, in drawing up a penal order regarding the coercive measure, may determine the recovery of money or restriction of rights as a coercive measure to a legal person. *[14 March 2013; 10 March 2016]*
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures	During the pre-trial criminal proceedings the investigator makes a decision on data preservation and sends it to Internet service provider (ISP) – Article 192 of the CPL. ISP then preserves required data for 30 days (or even more based on the decision of the investigating judge). The investigator than goes to the court with request to authorize data preservation. The investigating judge analyses all details of the case and makes a decision whether to authorize or to restrict data preservation. In case of a positive decision of an investigating judge, the investigator forwards the decision of the court to the ISP and receives saved data in return. Another option: During the pre-trial criminal proceedings an investigator with the consent of a public prosecutor or a data subject and a public prosecutor with the consent of a higher-ranking prosecutor or a data subject may request, that the merchant of an electronic information system disclose and issue the data to be stored (types of data – Electronic Communications Law, Art. 1, 2) in the information system in accordance with the procedures laid down in the Electronic Communications Law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	In accordance with the Latvian Criminal Procedure Law (CPL): **Section 191. Storage of Data located in an Electronic Information System** (1) The person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system. (2) The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days. **Section 192. Disclosure and Issue of Data Stored in an Electronic Information System** (1) During the pre-trial criminal proceedings an investigator with the consent of a prosecutor or a data subject and a prosecutor with the consent of a higher-ranking prosecutor or a data subject may request, that the merchant of an electronic information system disclose and issue the data to be stored in the information system in accordance with the procedures laid down in the Electronic Communications Law. (2) During the pre-trial criminal proceedings the person directing the proceedings may request in writing, on the basis of a decision of an investigating

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law. (3) In trying a criminal case, a judge or the court panel may request that a merchant of electronic communications discloses and issues the data to be stored in accordance with the procedures laid down in the Electronic Communications Law or that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	According to Article 12 of the Criminal Procedure Law "criminal proceedings shall be performed in conformity with internationally recognised civil rights and without allowing for the imposition of unjustified criminal procedural duties or excessive intervention in the life of a person" by further explaining that "civil rights may be restricted only in cases where such restriction is required for public safety reasons, and only in accordance with the procedures laid down in this Law according to the character and danger of the criminal offence". The article also states that "application of safety measures related to the deprivation of liberty, the infringement of the immunity of publicly inaccessible places, and the confidentiality of correspondence and means of communication shall be permitted only with the consent of the investigating judge or court". Furthermore, "an official, who performs the criminal proceedings, has a duty to protect the confidentiality of the private life of a person and the commercial confidentiality of a person" and that "information regarding such confidentiality shall be obtained and used only in the case where such information is necessary in order to clarify conditions that are to be proven". Finally, the article also states that "a natural person has the right to request that a criminal case does not include information regarding the private life, commercial activities, and financial situation of such person or the betrothed, spouse, parents,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	grandparents, children grandchildren, brothers or sisters of such person, as well as of the person with whom the relevant natural person is living together and with whom he or she has a common (joint) household, if such information is not necessary for the fair regulation of criminal legal relations".
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.	Data retention is covered in Section 190 of a Latvian Criminal Procedure Law (CPL). Section 190, Article 1 of CPL states that "person directing the proceedings, without conducting the seizure provided for in Section 186 of the Criminal Procedure Law, is entitled to request from natural or legal persons (for example Interned service providers), in writing, objects, documents and information regarding the facts that are significant to criminal proceedings, including in the form of electronic information and document that is processed, stored or transmitted using electronic information systems". Storage of data located in Electronic Information System is being regulated by Section 191 of the CPL, which states that "person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system". The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days. Retained and stored information is being issued to requesting party by International Cooperation Department of the Central Criminal Police Department within the State Police of the Republic of Latvia on the basis of October 5, 2006 Law On the Convention on Cybercrime and the Convention on Cybercrime Additional Protocol on combating racism and xenophobic crimes which are being committed through computer systems, in accordance to procedures laid down by Chapter II of the Law on the Exchange of Information for the Prevention of Criminal Offences. Based on Article 375 of the Criminal Procedure Law, Internet service provider is not allowed to disclose information related to received request on data

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	preservation within the framework of the criminal proceedings without the agreement of the body which requested data preservation.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Data retention is covered in Section 190 of a Latvian Criminal Procedure Law (CPL). Section 190, Article 1 of CPL states that "person directing the proceedings, without conducting the seizure provided for in Section 186 of the Criminal Procedure Law, is entitled to request from natural or legal persons (for example Interned service providers), in writing, objects, documents and information regarding the facts that are significant to criminal proceedings, including in the form of electronic information and document that is processed, stored or transmitted using electronic information systems". Storage of data located in Electronic Information System is being regulated by Section 191 of the CPL, which states that "person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system". The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days. Retained and stored information is being issued to requesting party by International Cooperation Bureau of the Central Criminal Police Department within the State Police of the Republic of Latvia on the basis of October 5, 2006 Law On the Convention on Cybercrime and the Convention on Cybercrime Additional Protocol on combating racism and xenophobic crimes which are being committed through computer systems, in accordance to procedures laid down

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	by Chapter II of the Law on the Exchange of Information for the Prevention of Criminal Offences. Based on Article 375 of the Criminal Procedure Law, Internet service provider is not allowed to disclose information related to received request on data preservation within the framework of the criminal proceedings without the agreement of the body which requested data preservation.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	Procedure according to Electronic Communication Law
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	Article 179 of the Criminal Procedure Law states that "search shall be conducted for the purpose of finding objects, documents, corpses, or persons being sought that are significant in criminal proceedings"; Articles 180-185 further specifies the procedure to be followed and other relevant issues. Article 186 states that "seizure is an investigative action whose content is the removal of objects or documents significant to a case, if the performer of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 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.	investigative action knows where or by whom the concrete object or document is located and a search for such object or document is not necessary, or such object or document is located in a publicly accessible place"; additional seizure related matters are regulated in Articles 187-188.
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	Control of means of communication (a special investigative action) Article 218 of the Criminal Procedure Law states that "the control of telephones and other means of communications without the knowledge of the members of a conversation or the sender and recipient of information shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the conversation or transferred information may contain information regarding facts included in circumstances to be proven, and if the acquisition of necessary information is not possible without such operation".

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	It further explains that "the control of telephones and other means of communication with the written consent of a member of a conversation, or the sender or recipient of information, shall be performed if there are grounds to believe that a criminal offence may be directed against such persons or the relative thereof, or also if such person is involved or may be enlisted in the committing of a criminal offence". Control of data located in automated data processing system (a special investigative action). Article 219 of the Criminal Procedure Law states that "search of an automated data processing system (a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the removal thereof without the information of the owner, possessor, or maintainer of such system or data shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the information located in the concrete system may contain information regarding facts included in circumstances to be proven". It further explains that "a person directing the proceedings may request, for the commencement of an investigative action, that the person who oversees the functioning of a system or performs duties related to data processing, storage or transmission provide the necessary information, ensure the completeness of the information and technical resources present in the system and make the data to be controlled unavailable to other users" and that "a person directing the proceedings may prohibit such person to perform other actions with data subject to control, as well as shall notify such person regarding the non-disclosure of an investigative secret". It is also clarified that "in a decision on control of data present in an automated data processing system an investigating judge may allow a person directing the proceedings to remove or store otherwise the resources of an automated data processing system, as well as to make copies of these resources". Control of the content of transmitted data (a special investigative action) Article 220 of the Criminal Procedure Law states that "the interception, collection and recording of data transmitted with the assistance of an automated data processing system using communication devices located in the territory of Latvia without the information of the owner, possessor, or maintainer of such system shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the information obtained from data

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	transmission may contain information regarding facts included in circumstances to be proven".
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.	Control of means of communication (a special investigative action) Article 218 of the Criminal Procedure Law states that "the control of telephones and other means of communications without the knowledge of the members of a conversation or the sender and recipient of information shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the conversation or transferred information may contain information regarding facts included in circumstances to be proven, and if the acquisition of necessary information is not possible without such operation". It further explains that "the control of telephones and other means of communication with the written consent of a member of a conversation, or the sender or recipient of information, shall be performed if there are grounds to believe that a criminal offence may be directed against such persons or the relative thereof, or also if such person is involved or may be enlisted in the committing of a criminal offence". Control of data located in automated data processing system (a special investigative action). Article 219 of the Criminal Procedure Law states that "search of an automated data processing system (a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the removal thereof without the information of the owner, possessor, or maintainer of such system or data shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the information located in the concrete system may contain information regarding facts included in circumstances to be proven". It further explains that "a person directing the proceedings may request, for the commencement of an investigative action, that the person who oversees the functioning of a system or performs duties related to data processing, storage or transmission provide the necessary information, ensure the completeness of the information and technical resources present in the system and make the data to be controlled unavailable to other users" and that "a person directing the proceedings may prohibit such person to perform other actions with data subject to control, as well as shall notify such person regarding the non-disclosure of an investigative secret". It is also clarified that "in a decision on control of data present in an automated data processing system an investigating judge may allow a person directing the

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	proceedings to remove or store otherwise the resources of an automated data processing system, as well as to make copies of these resources". Control of the content of transmitted data (a special investigative action) Article 220 of the Criminal Procedure Law states that "the interception, collection and recording of data transmitted with the assistance of an automated data processing system using communication devices located in the territory of Latvia without the information of the owner, possessor, or maintainer of such system shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the information obtained from data transmission may contain information regarding facts included in circumstances to be proven".
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,	According to Article 4 of the Criminal Law (on applicability of the Criminal Law outside the territory of Latvia) "Latvian citizens, non-citizens and foreigners who have a permanent residence permit for the Republic of Latvia, shall be held liable, in accordance with (..) [the Criminal] Law, in the territory of Latvia for an offence committed in the territory of another state or outside the territory of any state irrespective of whether it has been recognized as criminal and punishable in the territory of commitment". For an offence committed by a natural person "acting in the interests of a legal person registered in the Republic of Latvia, for the benefit of the person or as a result of insufficient supervision or control thereof in the territory of another state or outside the territory of any state irrespective of whether it has been recognized as criminal and punishable in the territory of commitment the legal person may be applied the coercive measures provided for in (..) [the Criminal] Law". It further explains that "foreigners who do not have permanent residence permits for the Republic of Latvia and who have committed serious or especially serious crimes in the territory of another state which have been directed against the Republic of Latvia or against the interests of its inhabitants, shall be held criminally liable in accordance with (..) [the Criminal] Law irrespective of the laws of the state in which the crime has been committed, if they have not been held criminally liable or committed to stand trial in accordance with the laws of the state where the crime was committed". Foreigners who do not have a permanent residence permit for the Republic of Latvia and "who have committed a criminal offence in the territory of another state or outside the territory of any state, in the cases provided for in international

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	agreements binding upon the Republic of Latvia, irrespective of the laws of the state in which the offence has been committed, shall be held liable in accordance with (..) [the Criminal] Law if they have not been held criminally liable for such offence or committed to stand trial in the territory of another state".
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence,	According to Section 682 of Criminal Procedure Law (Chapter 65. Extradition of a Person to Latvia) the extradition of a person may be requested, if there are grounds to believe that the following is located in a foreign state: a person who is a suspect or accused in the committing of a criminal offence that may be punished on the basis of The Criminal Law, and regarding which deprivation of liberty is intended with a maximum limit of not less than one year, if an international agreement does not provide for another term; or a person who has been convicted in Latvia with deprivation of liberty for a term of not less than four months. According to Section 696 of Criminal Procedure Law (Chapter 66. Extradition of a Person to a Foreign State) determines the grounds for the extradition of a person: a person who is located in the territory of Latvia may be extradited for criminal prosecution, trial, or the execution of a judgment, if a request has been received for temporary arrest or from a foreign state to extradite such person regarding an offence that, in accordance with the law of Latvia and the foreign state, is criminal; a person may be extradited for criminal prosecution, or trial, regarding an offence the committing of which provides for a punishment of deprivation of liberty the maximum limit of which is not less than one year, or a more serious punishment, if the international agreement does not provide otherwise; a person may be extradited for the execution of a judgment by the state that rendered the judgment and convicted the person with a punishment that is related to deprivation of liberty for a term of not less than four months, if the international agreement does not provide otherwise; if extradition has been requested regarding several criminal offences, but extradition may not be applied for one of such offences because such offence does not comply with the conditions regarding the possible or imposed punishment, the person may also be extradited regarding such criminal offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	Based on above mentioned, all cybercrime acts covered by the Criminal law (please, see answer to Q. 2.A.1) falls in the scope of the EAW (1. give rise to surrender; 2. are extraditable) as they are corresponding to Section 682 and Section 696 of the Criminal Procedure Law. The authority responsible for making or receiving requests for extradition or provisional arrests in the absence of a treaty is Prosecutor General Office.
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested	The competent institutions for mutual legal assistance in criminal matters are the State Police, General Prosecutor's Office and Ministry of Justice. Legal base: European Convention on Mutual Assistance in Criminal Matters of 20 April 1959; Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	The competent institutions to exchange spontaneous information are the State Police and General Prosecutor's Office Legal base: European Convention on Mutual Assistance in Criminal Matters of 20 April 1959; Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.	The authority responsible for sending and answering requests for mutual assistance the execution of such requests or their transmission to the authorities for their execution is Ministry of Justice

Back to the Table of Contents

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

Back to the Table of Contents

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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
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	Execution of an international request on data preservation is being made on the basis of an Article 192 of the CPL. Issuing an international request for data preservation in most cases is based on: - 1959 European Convention on Mutual Assistance in Criminal Matters; - May 29th, 2000, Council Act establishing, in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union; - COUNCIL ACT of 16 October 2001 establishing, in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union; - Convention on Cybercrime, Budapest, 23.XI.2001. In accordance to the article 5 of the "Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems", based on Article 35 of Schengen Convention, the relevant institution is the International Cooperation Bureau of the Central Criminal Police Department within the State Police of the Republic of Latvia Latvia reserves the right to refuse the request for preservation under this article where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall 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.	Disclosure of sufficient amount of traffic data is not specifically covered by the Latvian CPL, but Section 191 and 192 still apply.
Article 31 – Mutual assistance regarding accessing of stored computer data	According to Latvian Criminal Procedure Law' Section 192. Disclosure and Issue of Data Stored in an Electronic Information System

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(1) During the pre-trial criminal proceedings an investigator with the consent of a public prosecutor or a data subject and a public prosecutor with the consent of a higher-ranking prosecutor or a data subject may request, that the merchant of an electronic information system disclose and issue the data to be stored in the information system in accordance with the procedures laid down in the Electronic Communications Law. (2) During the pre-trial criminal proceedings the person directing the proceedings may request in writing, on the basis of a decision of an investigating judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law. (3) In trying a criminal case, a judge or the court panel may request that a merchant of electronic communications discloses and issues the data to be stored in accordance with the procedures laid down in the Electronic Communications Law or that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law. **Section 845. Grounds for the Assistance to a Foreign Country in the Performance of Procedural Actions** The grounds for procedural assistance are the following: 1) a request of a foreign country regarding the provision of assistance in the performance of a procedural action (hereinafter in this Chapter also - the request of a foreign country); 2) a decision of the competent authority of Latvia on admissibility of a procedural action.
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	According to Section 191 and 192 of the Criminal Procedure Law an investigator's decision for traffic data storage is needed and to disclosure and issue traffic data is necessary an investigating judge decision. The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days. **Section 845. Grounds for the Assistance to a Foreign Country in the Performance of Procedural Actions** The grounds for procedural assistance are the following: 1) a request of a foreign country regarding the provision of assistance in the performance of a procedural action (hereinafter in this Chapter also - the request of a foreign country); 2) a decision of the competent authority of Latvia on admissibility of a procedural action.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	According to Section 218, 219 and 220 of the Criminal Procedure Law for interception Content data is necessary an investigating judge decision. **Section 845. Grounds for the Assistance to a Foreign Country in the Performance of Procedural Actions** The grounds for procedural assistance are the following: 1) a request of a foreign country regarding the provision of assistance in the performance of a procedural action (hereinafter in this Chapter also - the request of a foreign country); 2) a decision of the competent authority of Latvia on admissibility of a procedural action.
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;	International Cooperation Deprtment (ICD) is a part of Central Criminal Police Department of the State Police of Latvia. The legal basis for operations of the State Police is the Constitution of the Republic of Latvia, international agreements, Law on Police, other laws and regulatory enactments of the Republic of Latvia, and decisions of local governments, if they are not contrary to the laws of the Republic of Latvia. Function of ICB which is dedicated to tackling cybercrime is based on 2001 Convention on Cybercrime and Directive 2013/40/EU of the European

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Parliament and of the Council of 12 August 2013 on attacks against information systems.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	Declarations made by Latvia can be found on home page of the convention https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=yu6JwkIq

Back to the Table of Contents