Finland

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**The Criminal Code: Chapter 38 - Data and communications offences** *Section 13 - Definitions* --- (2) When applying sections 3, 7(a) and 8, "data" refers also to the following, as referred to in article 2(a) of Directive 2013/40/EU of the Directive on Attacks against Information Networks: (1) a representation of facts, information or concepts in a form suitable for processing in an information system; and (2) a programme suitable for causing an information system to perform a function. **The Coercive Measures Act: Chapter 10 – Covert coercive means** *Section 6 – Traffic data monitoring and its prerequisites* (1)*Traffic data monitoring* refers to the obtaining of identifying data regarding a message that has been sent from or received by a network address or terminal end device connected to a telecommunications network referred to in section 3, the obtaining of location data regarding the network address or the terminal end device, or the temporary prevention of the use of the network address or terminal end device. *Identifying data* refers to data referred to in section 2, paragraph 8 of the Act on the Protection of Privacy in Electronic Communications that can be connected to the subscriber or user and that is processed in telecommunications networks in order to transmit or distribute messages or keep messages available. ---

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**The Criminal Code: Chapter 38 - Data and communications offences** *Section 8 - Computer break-in* (1) A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into an information system where information or data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a computer break-in to a fine or to imprisonment for at most two years. (2) Also a person who, without hacking into the information system or a part thereof, (1) by using a special technical device or (2) otherwise by by-passing the system of protection in a technical manner, by using a vulnerability in the information system or otherwise by evidently fraudulent means unlawfully obtains information or data contained in an information system referred to in subsection 1, shall be sentenced for a computer break-in. (3) An attempt is punishable. (4) This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law. *Section 8(a) – Aggravated computer break-in* (1) If the computer break-in is committed (1) as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2, or (2) in a particularly methodical manner

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and the computer break-in is aggravated also when assessed as a whole, the offender shall be sentenced for an aggravated computer break-in to a fine or to imprisonment for at most three years. **Declaration** Pursuant to Article 2 of the Convention, Finland has declared that it requires for the punishability of illegal access as referred to in the Article that the offence be committed by infringing security measures.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**The Criminal Code: Chapter 38 - Data and communications offences** *Section 3 - Message interception* (1) A person who unlawfully (1) opens a letter or another closed communication addressed to another or by hacking obtains information on the contents of an electronic or other technically recorded message which is protected from outsiders, or (2) obtains information on the contents of a telephone call, telegram, transmission of text, images or data, or another comparable telemessage transmitted by telecommunications or an information system or on the transmission or reception of such a message shall be sentenced for message interception to a fine or to imprisonment for at most two years. (2) An attempt is punishable. *Section 4 - Aggravated message interception* (1) If in the message interception (1) the offender commits the offence by making use of his or her position in the service of a telecommunications company, as referred in the Act on the Protection of Electronic Messages (516/2004) or his or her other special position of trust,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) the offender commits the offence by making use of a computer program or special technical device designed or altered for such purpose, or otherwise especially methodically, or (3) the message that is the object of the offence has an especially confidential content or the act constitutes a grave violation of the protection of privacy and the message interception is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated message interception to imprisonment for at most three years. (2) An attempt is punishable. See also Chapter 38, Section 8, Paragraph 2 (computer break-in) of the Finnish Criminal Code, see above.
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.	**The Criminal Code: Chapter 35 - Criminal damage** *Section 3(a) – Damage to data* (1) A person who, in order to cause damage to another, unlawfully destroys, demolishes, hides, damages, alters, renders unusable or conceals data recorded on an information device or another recording or data in an information system, shall be sentenced for damage do data to a fine or to imprisonment for at most two years. (2) An attempt is punishable. *Section 3(b) – Aggravated damage to data* (1) If the damage to data (1) causes particularly serious harm or economic loss, (2) is committed as part of the activity of an organised criminal group referred to in Chapter 6, section 5, subsection 2, (3) is committed as part of activity that has affected a significant amount of information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1,

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b), or (4) is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these, and the damage to data is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated damage to data to imprisonment for at least four months and at most five years. (2) An attempt is punishable. *Section 3(c) - Petty damage to data* If the damage to data, when assessed as a whole, with due consideration to the minor significance of the damage or the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for petty damage to data to 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	**The Criminal Code: Chapter 38 - Data and communications offences** *Section 5 – Interference with communications* (1) A person who by tampering with the operation of a device used in postal, telecommunications or radio traffic, by maliciously transmitting interfering messages over radio or telecommunications channels or in another comparable manner unlawfully prevents or interferes with postal, telecommunications or radio traffic, shall be sentenced for interference with communications to a fine or to imprisonment for at most two years. (2) An attempt is punishable. *Section 6 - Aggravated interference with communications* (1) If in the interference with communications

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) the offender commits the offence by making use of his or her position in the service of an institution referred to in the Telecommunications Act, a cable operator referred to in the Cable Transmission Act (307/1987) or a public broadcasting institution, or his or her other special position of trust, (2) the offence prevents or interferes with the radio transmission of distress signals or such other telecommunications or radio transmissions that are made in order to protect human life (3) the offence is committed as part of activity that has to a significant degree affected information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b), (4) the offence is committed as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2, (5) the offence causes particularly serious harm or economic loss, (6) the offence is directed at a device, information system or communications, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these, and the interference with communications is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated interference with communications to imprisonment for at least four months and at most five years. (2) An attempt is punishable. *Section 7 - Petty interference with communications* (1) If the interference with communications, in view of its nature or extent or the other circumstances of the offence, is of minor significance when assessed as a whole, the offender shall be sentenced for petty interference with communications to a fine. (2) An attempt is punishable.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section (7a) – Interference in an information system (1) A person who in order to cause detriment or economic loss to another, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of an information system or causes serious interference in it shall be sentenced for interference in an information system to a fine or to imprisonment for at most two years. (2) An attempt is punishable. *Section 7(b) – Aggravated interference in an information system* (1) If in the interference in an information system (1) particularly significant detriment or economic loss is caused, (2) the offence is committed in a particularly methodical manner, (3) the offence is committed as part of activity that has to a significant degree affected information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b), (4) the offence is committed as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2 or (5) the offence is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these, and the interference in an information system is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated interference in an information system to imprisonment for at least four months and at most five years. (2) An attempt is punishable.
Article 6 – Misuse of devices	**The Criminal Code: Chapter 34 – Endangerment**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	*Section 9(a) – Endangerment of data processing* A person who, in order to impede or damage data processing or the functioning or security of an information system or telecommunications system, (1) imports, obtains for use, manufactures, sells or otherwise disseminates or makes available (a) a device or computer program or set of programming instructions designed or altered to endanger or damage data processing or the functioning of an information system or telecommunications system or to break or disable the technical security of electronic communications or the security of an information system, or (b) an information system password, access code or other corresponding information belonging to another, or (2) disseminates or makes available instructions for the production of a computer program or set of programming instructions referred to in paragraph (1), shall be sentenced, unless an equally severe or more severe penalty for the act is provided elsewhere in the law, for endangerment of data processing to a fine or to imprisonment for at most two years. **The Criminal Code: Chapter 38 - Data and communications offences** *Section 8(b) — Offence involving a system for accessing protected services* A person who, in violation of the prohibition laid down in section 269, subsection 2 of the Information Society Code (917/2014), for commercial purposes or so that the act is conducive to causing considerable detriment or loss to a provider of protected services, produces, imports, offers for sale, rents out or distributes a system for accessing protected services, or advertises, installs or maintains the same, shall, unless a more severe or equally severe penalty is provided elsewhere in law for the act, be sentenced for an *offence involving a system for accessing protected services* to a fine or to imprisonment for at most one year.
Title 2 – Computer-related offences	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**The Criminal Code: Chapter 33 - Forgery offences** *Section 1 – Forgery* (1) A person who prepares a false document or other item or falsifies such a document or item in order for it to be used as misleading evidence or uses a false or falsified item as misleading evidence shall be sentenced for forgery to a fine or imprisonment for at most two years. (2) An attempt is punishable. *Section 2 - Aggravated forgery* (1) If in the forgery (1) the item that is the object of the offence is an archival document stored by an authority or a general register kept by an authority and such a document or register is important from a general point of view, or the item otherwise has a particularly significant probative value, or (2) the offender uses technical equipment procured for the commission of forgery offences or otherwise acts in a particularly methodical manner and the forgery is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated forgery to imprisonment for at least four months and at most four years. (2) An attempt is punishable. *Section 3 - Petty forgery* If the forgery, when assessed as a whole, with due consideration to the nature of the item or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for petty forgery to a fine. *Section 6 – Definitions*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) For the purposes of this Code, item refers to a document and its facsimile, a mark, a stamp, license plate, audio or video recording, a recording produced by a plotter, calculator or other comparable technical device and a recording that is suitable for data processing, if it is used or can be used as legally relevant evidence of rights, duties or facts. (2) An item is false if, when used as evidence, it is conducive to giving a misleading conception of its origin or of the identity of the person who issued it. (3) An item is falsified if its contents have been unlawfully altered in respect of a datum that has probative relevance.
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 Criminal Code: Chapter 36 - Fraud and other dishonesty** *Section 1 – Fraud (see paragraph 2)* (1) A person who, in order to obtain unlawful financial benefit for himself or herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for fraud to a fine or to imprisonment for at most two years. (2) Also a person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be sentenced for fraud. (3) An attempt is punishable. *Section 2 - Aggravated fraud* (1) If the fraud (1) involves the seeking of considerable benefit, (2) causes considerable or particularly significant loss,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) is committed by taking advantage of special confidence based on a position of trust or (4) is committed by taking advantage of a special weakness or other insecure position of another and the fraud is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated fraud to imprisonment for at least four months and at most four years. (2) An attempt is punishable. *Section 3 - Petty fraud* If the fraud, when assessed as a whole, with due consideration to the benefit sought or the amount of loss caused or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for petty fraud to a fine. **The Criminal Code: Chapter 37 - Means of payment offences** *Section 8 - Means of payment fraud* (1) A person who, in order to obtain unlawful economic benefit for himself or herself or another (1) uses a means of payment without the permission of the lawful holder, in excess of his or her right based on such permission, or otherwise without lawful right, or (2) transfers a means of payment or means of payment form to another in order to have it used without lawful right shall be sentenced for means of payment fraud to a fine or to imprisonment for at most two years. (2) Also a person who, by overdrawing his or her account or exceeding the agreed maximum credit limit, misuses a means of payment referred to in subsection 1 and in this way causes economic loss to another shall be sentenced

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for means of payment fraud, unless when using the means of payment he or she intended to compensate the loss without delay. *Section 9 - Aggravated means of payment fraud* If in the means of payment fraud (1) considerable or particularly significant loss is caused or (2) the offender has, for the commission of the offence, made or had made means of payment forms from which the means of payment used in the offence was prepared, or if the offence is otherwise committed in a particularly methodical manner and the means of payment fraud is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated means of payment fraud to imprisonment for at least four months and at most four years. *Section 10 - Petty means of payment fraud* If the means of payment fraud, when assessed as a whole, with due consideration to the amount of benefit sought or the amount of loss caused or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for petty means of payment fraud to a fine.
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;	**The Criminal Code: Chapter 17 - Offences against public order** *Section 18 - Distribution of a sexually offensive picture* (1) A person who manufactures, offers for sale or for rent or otherwise offers or makes available, keeps available, exports, imports to or transports through Finland to another country, or otherwise distributes pictures or visual recordings that factually or realistically depict (1) a child, (2) violence or (3) bestiality

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	shall be sentenced for distribution of a sexually offensive picture to a fine or imprisonment for at most two years. (2)An attempt is punishable. (3) The provisions in section 17, subsection 2 apply also to the pictures and visual recordings referred to in this section. (4) A child is defined as a person below the age of eighteen years and a person whose age cannot be determined but whom there is justifiable reason to assume is below the age of eighteen years. The picture or visual recording is deemed factual in the manner referred to in subsection 1, paragraph 1, if it has been produced in a situation in which a child has actually been the object of sexually offensive conduct and realistic, if it resembles in a misleading manner a picture or a visual recording produced through photography or in another corresponding manner of a situation in which a child is the object of sexually offensive conduct. The definitions of the terms factual and realistic apply correspondingly in the cases referred to in subsection 1, paragraphs 2 and 3. *Section 18(a) - Aggravated distribution of a sexually offensive picture depicting a child* (1) If, in the distribution of a sexually offensive picture depicting a child (1) the child is particularly young, (2) the picture also depicts severe violence or particularly humiliating treatment of the child, (3) the offence is committed in a particularly methodical manner or (4) the offence has been committed within the framework of an organized criminal group referred to in Chapter 6, section 5, subsection 2 and the offence is aggravated also when assessed as whole, the offender shall be sentenced for aggravated distribution of a sexually offensive picture depicting a child to imprisonment for at least four months and at most six years. (2) An attempt is punishable.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 19 - Possession of a sexually offensive picture depicting a child (1) A person who unlawfully has in his or her possession a picture or visual recording which depicts a child in the sexually offensive manner referred to in section 18, shall be sentenced for possession of a sexually offensive picture depicting a child to a fine or to imprisonment for at most one year. (2) A person who in return for payment or otherwise by agreement has obtained access to a picture or visual recording referred to in subsection 1 so that it is available to him or her on a computer or another technical device without being recorded on the device shall also be sentenced for possession of a sexually offensive picture depicting a child.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other	**The Criminal Code: Chapter 49 - Violation of certain incorporeal rights** *Section 1 - Copyright offence* (1) A person who for profit and in violation of the Copyright Act (404/1961) and in a manner conducive to causing considerable detriment or damage to the person holding a right, violates the right of another to (1) a literary or artistic work, (2) the performance of a literary or artistic work or of national heritage, (3) a record or other device on which sound has been recorded, (4) a film or other device on which moving images have been recorded, (5) a television or radio broadcast, (6) a register, table, program or another similar work referred to in the Copyright Act and containing the compilation of a considerable amount of information, or a database the compilation, verification or presentation of which has required considerable effort, or (7) a photograph shall be sentenced for a copyright offence to a fine or to imprisonment for at most two years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) Also a person who for profit and in a manner conducive to causing considerable detriment or damage to the person holding a right, imports for the purpose of dissemination among the public or for transport through Finland to a third state a sample or a copy produced abroad of a work or photograph, a record, film or other device on which sound or moving pictures have been recorded or a register, table, program or another similar work containing the compilation of a consider-able amount of information, or a database the compilation, verification or presentation of which has required considerable effort, as referred to in subsection 1, while knowing that it has been produced or copied in circumstances under which said production or copying would in Finland be punishable under subsection 1 or under section 56(a) of the Copyright Act, shall be sentenced for a copyright of-fence. (3) Also a person who uses a computer network or information system to violate the right of another to the objects of protection referred to in subsection 1 so that the act is conducive to causing considerable detriment or damage to the holder of the right that has been violated, shall be sentenced for a copyright offence. **The Copyright Act** *Section 56a – Copyright violation* (1) Anyone who 1. wilfully or out of gross negligence makes a copy of a work, or makes a work available to the public contrary to the provisions of this Act or infringes the provisions of section 3 concerning moral rights, 2. otherwise violates a provision protecting copyright in the present Act or acts contrary to a direction issued under section 41(2), or to a provision of section 51 or section 52, or to a prohibition referred to in section 53(1) or section 54b(1), or 3. imports into the country or brings onto the territory of Finland for transportation to a third country copies of a work which he knows or has well founded reason to suspect to have been produced outside the country under such circumstances that such production in Finland would have been punishable under this Act, shall be sentenced to a fine for a copyright violation, unless the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	act is punishable as a copyright offence under section 1 of Chapter 49 of the Penal Code. (2) The making of single copies for private use of a computer-readable computer program or a database which has been published or copies of which have been sold or otherwise permanently transferred with the consent of the author, or the making of single copies for private use of a work contrary to section 11(5) shall not be considered to constitute a copyright violation.
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.	**The Criminal Code: Chapter 5 – On attempt and complicity** *Section 1 - Attempt* (1) An attempt of an offence is punishable only if the attempt has been denoted as punishable in a provision on an intentional offence. (2) An act has reached the stage of an attempt at an offence when the perpetrator has begun the commission of an offence and brought about the danger that the offence will be completed. An attempt at an offence is involved also when such a danger is not caused, but the fact that the danger is not brought about is due only to coincidental reasons. (3) In sentencing for an attempt at an offence, the provisions of chapter 6, section 8, subsection 1(2), subsection 2 and subsection 4 apply, unless, pursuant to the criminal provision applicable to the case, the attempt is comparable to a completed act. *Section 6 – Abetting* (1) A person who, before or during the commission of an offence, intentionally furthers the commission by another of an intentional act or of its punishable attempt, through advice, action or otherwise, shall be sentenced for abetting on the basis of the same legal provision as the perpetrator. The provisions of Chapter 6, section 8, subsection 1(3), subsection 2 and subsection 4 apply nonetheless to the sentence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2)Incitement to punishable aiding and abetting is punishable as aiding and abetting. --- According to the Criminal Code provisions related to Articles 2 to 10 attempts of the following offences are punishable: - computer break-in, - aggravated computer break-in, - message interception, - aggravated message interception, - damage to data, - aggravated damage to data, - interference with communications, - aggravated interference with communications, - petty interference with communications, - interference in an information system, - aggravated interference in an information system, - forgery, - aggravated forgery, - fraud, - aggravated fraud, - distribution of a sexually offensive picture and - aggravated distribution of a sexually offensive picture depicting a child. Because offences related to Articles 2 to 10 are intentional aiding/abetting the commission of all offences connected with the Convention is punishable (Chapter 5, section 6 of the Criminal Code). **Declaration** Pursuant to Article 11, paragraph 3, of the Convention, Finland has declared that it will not apply paragraph 2 of the same article, concerning the criminalisation of attempt, to petty criminal damage nor petty forgery.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**The Criminal Code: Chapter 9 – Corporate criminal liability** *Section 1 - Scope of application* (1) A corporation, foundation or other legal entity (corporation) in the operations of which an offence has been committed shall on the request of the public prosecutor be sentenced to a corporate fine if such a sanction has been provided in this Code for the offence. (2) The provisions in this Chapter do not apply to offences committed in the exercise of public authority. *Section 2 - Prerequisites for liability* (1) A corporation may be sentenced to a corporate fine if a person who is part of its statutory organ or other management or who exercises actual decision-making authority therein has been an accomplice in an offence or allowed the commission of the offence or if the care and diligence necessary for the prevention of the offence have not been observed in the operations of the corporation. (2) A corporate fine may be imposed even if the offender cannot be identified or otherwise is not punished. However, no corporate fine shall be imposed for a complainant offence which is not reported by the injured party so as to have charges brought, unless there is a very important public interest for the bringing of charges. *Section 3 - Connection between offender and corporation* (1) The offence is deemed to have been committed in the operations of a corporation if the perpetrator has acted on the behalf or for the benefit of the corporation, and belongs to its management or is in a service or employment relationship with it or has acted on assignment by a representative of the corporation.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) The corporation does not have the right to compensation from the offender for a corporate fine that it has paid, unless such liability is based on statutes on corporations and foundations. --- Corporate criminal liability covers following offences related to the Convention: - distribution of a sexually offensive picture, aggravated distribution of a sexually offensive picture depicting a child and possession of a sexually offensive picture depicting a child (Chapter 17, section 24(1) of the Criminal Code), - forgery and aggravated forgery (Chapter 33, section 7 of the Criminal Code), - endangerment of data processing (Chapter 34, section 13 of the Criminal Code), - damage to data and aggravated damage to data (Chapter 35, section 8 of the Criminal Code), - fraud deferred to in Chapter 36, section 1(2) of the Criminal Code and aggravated fraud when it has been committed in the manner provided in Chapter 36, section 1(2) of the Criminal Code (Chapter 36, section 9 of the Criminal Code), - means of payment fraud and aggravated means of payment fraud (Chapter 37, section 14 of the Criminal Code), - message interception, aggravated message interception, interference with communications, aggravated interference with communications, interference in an information system, aggravated interference in an information system, computer break-in and aggravated computer break-in (Chapter 38, Section 12 of the Criminal Code). According to the Section 3(1) of the Tort Liability Act (412/1974) an employer is liable for damages caused by an employee through an error or negligence at work. This liability may materialise in cases where an employee has caused damages by committing offence/offences, including offences in question.
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	According to the Criminal Code provisions penalty scales of the offences in question are as follows:

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	- computer break-in: a fine or imprisonment for at most two years, - aggravated computer break-in: a fine or imprisonment for at most three years, - message interception: a fine or imprisonment for at most two years, - aggravated message interception: imprisonment for at most three years, - damage to data: a fine or imprisonment for at most two years, - aggravated damage to data: to imprisonment for at least four months and at most five years, - petty damage to data: a fine, - interference with communications: a fine or imprisonment for at most two years, - aggravated interference with communications: imprisonment for at least four months and at most five years, - petty interference with communications: a fine, - interference in an information system: a fine or imprisonment for at most two years, - aggravated interference in an information system: imprisonment for at least four months and at most five years, - endangerment of data processing: a fine or imprisonment for at most two years, - offence involving a system for accessing protected services: a fine or imprisonment for at most one year, - forgery: a fine or imprisonment for at most two years, - aggravated forgery: imprisonment for at least four months and at most four years, - petty forgery: a fine, - fraud: a fine or imprisonment for at most two years, - aggravated fraud: imprisonment for at least four months and at most four years, - petty fraud: a fine, - means of payment fraud: a fine or imprisonment for at most two years, - aggravated means of payment fraud: imprisonment for at least four months and at most four years, - petty means of payment fraud: a fine, - distribution of a sexually offensive picture: a fine or imprisonment for at most two years,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- aggravated distribution of a sexually offensive picture depicting a child: imprisonment for at least four months and at most six years, - possession of a sexually offensive picture depicting a child: a fine or to imprisonment for at most one year, - copyright offence: a fine or to imprisonment for at most two years and - copyright violation: a fine. **The Criminal Code: Chapter 9 – Corporate criminal liability** *Section 5 - Corporate fine* A corporate fine is imposed as a lump sum. The corporate fine is at least 850 euros and at most 850,000 euros.
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	**The Coercive Measures Act** Coercive Measures Act covers following measures: - apprehension, arrest and remand (Chapters 2 and 3), - restriction of contacts (Chapter 4) - travel ban (Chapter 5), - seizure for security for the payment of a fine, of compensation or restitution or of an amount to be declared to forfeited to the state (Chapter 6), - seizure and copying of a document (Chapter 7), - search (Chapter 8; search of premises, search of a technical device and personal search), - coercive measures related to special investigative means (Chapter 9; cordoning off the site or the object of an investigation, test to determine the consumption of alcohol or other intoxicating substance, taking of personal identifying characteristics and preparation and recording of DNA profiles) and - covert (secret) coercive means (Chapter 10; telecommunications interception, traffic data monitoring, obtaining location data, obtaining base station data, extended surveillance, covert collection

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	of intelligence, on-site interception, technical observation, technical monitoring, technical surveillance of a device, covert activity, pseudo-purchase, use of covert human intelligence and controlled delivery). Conditions on the use of coercive measures are regulated in the provisions related to the measure in question. The object of the measure is usually a suspected person, the purpose of the measure is usually clearing on offence and usually decisive is the seriousness of the offence. Some measures are available in the investigation of all offences. Concerning covert coercive means provisions include some measure-tied extra conditions like "particularly important significance in the clarification of an offence" or "necessary for the clarification of an offence". **Declarations** Pursuant to Article 14, paragraph 3.a, of the Convention, Finland has declared that it only applies Article 20 to offences aimed at a computer system committed by using telecommunications terminal equipment, pandering, threatening of persons to be heard in the administration of justice, menace, narcotic offences or attempts of the above, preparation of offences to be committed with terrorist intent and offences punishable by imprisonment of at least four years. Pursuant to Article 14, paragraph 3.b, of the Convention, the Finland has declared that it does not apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system if the system is being operated for the benefit of a closed group of users and does not employ public communications networks and is not connected with another computer system, whether public or private.
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	Legislative measures concerning cybercrime offences have been carried out in a way that respects human rights and fundamental freedoms and the rule of law. Coercive measures used in criminal investigations interfere in human rights and fundamental freedoms in ways depending on the nature of the measure in question.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Measures deeply interfering with human rights and fundamental freedoms are usually allowed only in investigations of serious offences and a district court decides on the use of these measures (for example remand, seizure for security and many covert coercive measures). If the measure has been ordered by the police official or the prosecutor on the request of the person concerned in the matter the court shall decide whether the measure is to remain in force (for example travel ban and seizure and copying of document in many cases). If the measure has been ordered by the court on the request of the person concerned in the matter the court shall reconsider whether the measure is to remain in force. All coercive measure court decisions are covered either by the possibility to make an (ordinary) appeal (for example seizure for security and seizure and copying of document) or by the possibility to make an extraordinary appeal (no time limit and an urgent hearing; for example remand and travel ban). When a person subjected to a covert coercive measure is afterwards reported the use of measure he or she may make an extraordinary appeal. Certain principles have to be taken into account in the decision making concerning the use of all coercive measures. According to principle of proportionality manifested in Chapter 1, section 2 of the Coercive Measures Act coercive measures may be used only when they may be deemed justifiable with consideration to the seriousness of the offence under investigation, the importance of clarifying the offence, the degree to which the use of the coercive measures infringes on the rights of the suspect in the offence or others, and the other circumstances in the case. According to Chapter 1, Section 3(1) of the Coercive Measures Act (principle of minimum intervention) the use of a coercive measure may not infringe on the rights of anyone beyond what is necessary in order to achieve the purpose for which it is used.
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.	**The Coercive Measures Act: Chapter 8 – Search** *Section 24 – Data retention order* (1) If, before the search of data contained in a device, there is reason to assume that data that may be of significance for the clarification of the offence is deleted or is changed, an official with the power of arrest may issue a data retention order. Such an order requires that a person holding or administering data, not however the suspect in an offence, maintains the data unchanged.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	The order may apply also to data that can be assumed to be transmitted to a device or information system within the month following the issuing of the order. On request a written certificate shall be given of the order, detailing the data that is the object of the order. (2) What is provided in subsection 1 applies also to data in a message transmitted by an information system that relates to the origin, destination, routing and size of the message as well as to the time, duration, nature and other corresponding factors of the transmission (*transmission information*). (3) A criminal investigation authority does not, on the basis of the retention order referred to in subsection 1, have the right to obtain information on the contents of the message, transmission information or other recorded information. If several service providers have participated in the transmission of the message referred to in subsection 2, a criminal investigation authority has the right to obtain the transmission information necessary to identify the service providers. *Section 25 – Period of validity of a data retention order* A data retention order is issued for three months at a time. The order may be renewed when required by the investigation of the offence. The order shall be rescinded as soon as it is no longer necessary. *Section 26 – Secrecy of a data retention order* (1) A person who has received a data retention order is obliged to keep the order secret. (2) The punishment for violation of the obligation of secrecy in respect of a data retention order is imposed in accordance with Chapter 38, section 1 or 2 of the Criminal Code, unless a more severe punishment is provided elsewhere in law for the act.
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:	**The Coercive Measures Act: Chapter 8 –Search** *Section 24 – Data retention order*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(1) If, before the search of data contained in a device, there is reason to assume that data that may be of significance for the clarification of the offence is deleted or is changed, an official with the power of arrest may issue a data retention order. Such an order requires that a person holding or administering data, not however the suspect in an offence, maintains the data unchanged. The order may apply also to data that can be assumed to be transmitted to a device or information system within the month following the issuing of the order. On request a written certificate shall be given of the order, detailing the data that is the object of the order. (2) What is provided in subsection 1 applies also to data in a message transmitted by an information system that relates to the origin, destination, routing and size of the message as well as to the time, duration, nature and other corresponding factors of the transmission (*transmission information*). (3) A criminal investigation authority does not, on the basis of the retention order referred to in subsection 1, have the right to obtain information on the contents of the message, transmission information or other recorded information. If several service providers have participated in the transmission of the message referred to in subsection 2, a criminal investigation authority has the right to obtain the transmission information necessary to identify the service providers. *Section 25 – Period of validity of a data retention order* A data retention order is issued for three months at a time. The order may be renewed when required by the investigation of the offence. The order shall be rescinded as soon as it is no longer necessary. *Section 26 – Secrecy of a data retention order* (1) A person who has received a data retention order is obliged to keep the order secret. (2) The punishment for violation of the obligation of secrecy in respect of a data retention order is imposed in accordance with Chapter 38, section 1 or 2 of the Criminal Code, unless a more severe punishment is provided elsewhere in law for the act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	The Coercive Measures Act: Chapter 10 – Covert coercive means *Section 6 – Traffic data monitoring and its prerequisites* (1) *Traffic data monitoring* refers to the obtaining of identifying data regarding a message that has been sent from or received by a network address or terminal end device connected to a telecommunications network referred to in section 3, the obtaining of location data regarding the network address or the terminal end device, or the temporary prevention of the use of the network address or terminal end device. *Identifying data* refers to data referred to in section 2, paragraph 8 of the Act on the Protection of Privacy in Electronic Communications that can be connected to the subscriber or user and that is processed in telecommunications networks in order to transmit or distribute messages or keep messages available. (2) A criminal investigation authority may be issued a warrant for traffic data monitoring of a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect said person of: (1) an offence for which the most severe punishment is imprisonment for at least four years; (2) an offence committed with the use of the network address or terminal end device, for which the most severe punishment provided is imprisonment for at least two years; (3) unauthorized use directed at an automatic data processing system and committed with the use of a network address or terminal end device; (4) exploitation of a person subjected to the sex trade, solicitation of a child for sexual purposes or pandering; (5) a narcotics offence; (6) preparation of an offence committed with terrorist intent, training for the preparation of a terrorist offence or financing of a terrorist group; (7) an aggravated customs offence; (8) aggravated concealment of illegally obtained goods; (9) preparation of the taking of a hostage; or (10) preparation of aggravated robbery. (3) Section 17 of the Act on the Exercise of the Freedom of Speech in Mass

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Communications (460/2003) contains provisions on the transfer of identifying data concerning an electronic message.
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.	**The Criminal Investigation Act: Chapter 7 – Questioning** *Section 8 – The obligation of a witness to provide evidence and refusal to testify* --- (3) A witness is also required to produce a document or other evidence in his or her possession that is of significance for the criminal investigation, if it could be confiscated in accordance with Chapter 7, section 1 of the Coercive Measures Act and there are no bars to confiscation as provided in section 3 of said Chapter. --- *Section 9 – The questioning of a witness in court* (1) If a witness obviously knows of a circumstance that is important for the determination of guilt or for the tracing and seizing of the proceeds of an offence, and he or she refuses to reveal it even if he or she may be obliged to reveal it, the question of the grounds for refusal shall on the request of the head investigator be examined in court. The questioning of the witness shall be conducted in court if there is no lawful justification for the refusal. (2) What is provided in subsection 1 applies also to a witness who refuses to produce a document or other evidence. --- Subscriber and contact information are available to everyone unless they are confidential based on the wish of the customer and the agreement between him/her and the service provider. Operators produce as commercial services public directories of subscriber and contact information related to the telecommunication connections. These services are open sources. Not listed network addresses are covered by Chapter 4, section 3 of the Police Act:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	The Police Act: Chapter 4 - Technical monitoring and rights to information *Section 3 - Obtaining information from a private organisation or person* (1) At the request of a commanding police officer, the police has the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members and employees of an organisation. The police have the same right to obtain information needed in a police investigation referred to in Chapter 6 if an important public or private interest so requires. (2) In individual cases, the police has the right to obtain from a telecommunications operator and a corporate or association subscriber on request contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties. Similarly, the police has the right to obtain postal address information from organisations engaged in postal services. (3) For licence administration purposes, the police have the right to obtain information from private organisations and persons as provided in section 2(2–3).
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have	**The Coercive Measures Act: Chapter 8 – Search** *Section 20 – Definition of a search of data contained in a device* (1) A *search of data contained in a device* refers to a search that is directed at the data that is contained at the time of the search in a computer, a terminal end device or in another corresponding technical device or information system. (2) A search of data contained in a device may not be directed at a confidential message, in respect of which Chapter 10 contains provisions on telecommunications interception, traffic data monitoring and technical surveillance.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	*Section 21 – Prerequisites for a search of data contained in a device* (1) A search of data contained in a device may be conducted if: (1) there is reason to suspect that an offence has been committed and the most severe punishment provided for the offence is imprisonment for at least six months, or if the matter being investigated involves circumstances connected to the imposition of a corporate fine; and (2) it may be presumed that the search can lead to the discovery of a document or data to be seized as referred to in Chapter 7, section 1, subsections 1 or 2 or to a document to be copied on the basis of Chapter 7, section 2, and that is connected with the offence under investigation. (2) A search of data contained in a device may also be conducted in order to return the device to a person entitled to it, if there are grounds to suspect that it has been taken from someone by an offence. (3) The decision on the conduct of a search of the premises may be extended to cover also a technical device or information system in said premises, if the search in question is not one intended to find a person. **The Coercive Measures Act: Chapter 10 – Covert coercive means** *Section 23 – Technical surveillance of a device and its prerequisites* (1) The *technical surveillance of a device* refers to other than solely sensory surveillance, recording or other processing of the operation of a computer or other corresponding technical device or of the data or identification data contained therein, for the purpose of the investigation of a factor that is of significance for the clarification of an offence. (2) Technical surveillance of a device may not be used to obtain information about the content of a message or the identifying data referred to in section 6, subsection 1.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) The criminal investigation authority may direct technical surveillance of a device at a computer or another corresponding technical device or its program referred to in subsection 1 that is probably used by the suspect of an offence, when there are grounds to suspect this person of an offence referred to in section 16, subsection 3. **The Coercive Measures Act: Chapter 7 – Seizure and copying of a document** *Section 1 – Prerequisites for seizure* (1) An object, property or document may be seized if there are grounds to suspect that: (1) it may be used as evidence in a criminal case; (2) it has been taken from someone in an offence; or (3) it may be ordered forfeited. (2) What is provided in subsection 1, paragraphs 1 and 2 also applies to information that is contained in a technical device or in another corresponding information system or in its recording platform (*data*). The provisions in this Chapter regarding a document apply also to a document that is in the form of data. (3) The provisions in this Chapter on an object apply also to a substance. Part of an object may be detached from it to be used as evidence, if the investigative measure cannot otherwise be performed without considerable difficulties. *Section 2 – Copying of a document* (1) Seizure of a document to be used as evidence in accordance with section 1, subsection 1, paragraph 1 shall be replaced by copying of said document if a copy is sufficient from the point of view of the credibility of testimony. (2) A document shall be copied without undue delay after possession has been taken of it. After being copied it shall be returned without delay to the person from whom it was taken. (3) If a document cannot be copied without delay due to the nature or extent of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the document or documentation, the document shall be seized.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**The Coercive Measures Act: Chapter 10 – Covert coercive measures** *Section 6 – Traffic data monitoring and its prerequisites* (1) *Traffic data monitoring* refers to the obtaining of identifying data regarding a message that has been sent from or received by a network address or terminal end device connected to a telecommunications network referred to in section 3, the obtaining of location data regarding the network address or the terminal end device, or the temporary prevention of the use of the network address or terminal end device. *Identifying data* refers to data referred to in section 2, paragraph 8 of the Act on the Protection of Privacy in Electronic Communications that can be connected to the subscriber or user and that is processed in telecommunications networks in order to transmit or distribute messages or keep messages available. (2) A criminal investigation authority may be issued a warrant for traffic data monitoring of a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect said person of: (1) an offence for which the most severe punishment is imprisonment for at least four years; (2) an offence committed with the use of the network address or terminal end device, for which the most severe punishment provided is imprisonment for at least two years; (3) unauthorized use directed at an automatic data processing system and committed with the use of a network address or terminal end device; (4) exploitation of a person subjected to the sex trade, solicitation of a child for sexual purposes or pandering; (5) a narcotics offence; (6) preparation of an offence committed with terrorist intent, training for the preparation of a terrorist offence or financing of a terrorist group; (7) an aggravated customs offence; (8) aggravated concealment of illegally obtained goods; (9) preparation of the taking of a hostage; or (10) preparation of aggravated robbery.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Section 17 of the Act on the Exercise of the Freedom of Speech in Mass Communications (460/2003) contains provisions on the transfer of identifying data concerning an electronic message. *Section 7 – Traffic data monitoring with the consent of the possessor of a network address or terminal end device* (1) A criminal investigation authority may, with the consent of the suspect of an offence, the injured person, a witness or another person, monitor direct traffic at a network address or terminal end device in the possession of such person, when there are grounds to suspect: (1) an offence for which the most severe punishment is imprisonment for at least two years; (2) an offence as a result of which a network address or terminal end device is unlawfully in the possession of another person; (3) a violation of a restraint order, criminal mischief referred to in Chapter 17, section 13, paragraph 2 of the Criminal Code or violation of the privacy of telecommunications referred to in Chapter 24, section 1(a) of the Criminal Code, committed with the aid of a network address or terminal end device; (4) an offence committed with the aid of a network address or terminal end device, other than one referred to in paragraph 3; or (5) abuse of a victim of prostitution. (2) If the criminal investigation concerns an offence as a result of which a person has been killed, traffic data monitoring directed at a network address or terminal end device that had been in his or her possession does not require the consent of the legal successor of the person who has been killed. *Section 9 – The warrant for traffic data monitoring and for obtaining location data* --- (3) The warrant may be issued and the decision may be made for at most one month at a time and the warrant or decision may be issued to extend also to the period prior to the issuing of the warrant or the making of the decision, which may be longer than one month. ---
Article 21 – Interception of content data	**The Coercive Measures Act: Chapter 10 – Covert coercive measures**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	*Section 3 – Telecommunications interception and its prerequisites* (1) *Telecommunications interception* refers to the monitoring, recording and other processing of a message sent to or transmitted from a network address or terminal end device through a public communications network referred to in the Telecommunications Services Act or a communications network connected thereto, in order to determine the contents of the message and the identifying data connected to it referred to in section 6. Telecommunications interception may be directed only at a message that originates from or is intended for a suspect in an offence. (2) A criminal investigation authority may receive permission for telecommunications interception directed at a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect him or her of: (1) genocide, preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, torture, violation of a prohibition against chemical weapons, violation of a prohibition against biological weapons, violation against a prohibition against anti-infantry mines; (2) endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage, disclosure of a national secret, unlawful gathering of intelligence; (3) high treason, aggravated high treason, preparation of high treason; (4) aggravated distribution of a sexually offensive picture depicting a child; (5) sexual abuse of a child, aggravated sexual abuse of a child; (6) manslaughter, murder, homicide, preparation of an aggravated offence directed against life or health as referred to in Chapter 21, section 6a of the Criminal Code and in accordance with sections 1, 2 and 3 of said Chapter; (7) arrangement of aggravated illegal entry into the country, aggravated deprivation of liberty, trafficking in persons, aggravated trafficking in persons, kidnapping, preparation of kidnapping; (8) aggravated robbery, preparation of aggravated robbery, aggravated extortion; (9) aggravated concealment of illegally obtained goods, professional concealment of illegally obtained goods, aggravated money laundering;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(10) criminal mischief, criminal traffic mischief, aggravated sabotage, aggravated endangerment of health, a nuclear device offence, hijacking; (11) an offence committed with terrorist intent, preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence, financing of terrorism, as referred to in Chapter 34(a), section 1, subsection 1, paragraphs 2-7 or subsection 2 of the Criminal Code; (12) aggravated damage to property or aggravated damage to data; (13) aggravated fraud, aggravated usury; (14) aggravated counterfeiting; (15) aggravated impairment of the environment; or (16) an aggravated narcotics offence. (3) A warrant for telecommunications interception may be issued also when there are grounds to suspect a person of the following in connection with commercial or professional activity: (1) aggravated giving of a bribe; (2) aggravated embezzlement; (3) aggravated tax fraud, aggravated assistance fraud; (4) aggravated forgery; (5) aggravated dishonesty by a debtor, aggravated dishonesty by a debtor; (6) aggravated taking of a bribe, aggravated abuse of public office; (7) aggravated regulation offence; (8) aggravated abuse of insider information, aggravated market distortion; or (9) an aggravated customs offence. (4) An additional prerequisite to the issuing of the warrant referred to above in subsection 3 is that the offence was committed in order to obtain especially large benefit and the offence has been committed in an especially methodical manner. (5) A warrant for telecommunications interception may also be issued if there are grounds to suspect someone of aggravated pandering in which especially large benefit is sought and the offence has been committed in an especially

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	methodical manner or the offence is one referred to in Chapter 20, section 9(a), subsection 1, paragraph 3 of the Criminal Code. *Section 4 – The obtaining of information other than through telecommunications interception* (1) If it is probable that the message referred to in section 3 and the identifying data connected with it are no longer available through telecommunications interception, the criminal investigation authority may be granted permission, notwithstanding the prohibition in Chapter 7, section 4, and subject to the prerequisites provided in section 3, to confiscate or copy these from the possession of a telecommunications operator or a corporate or association subscriber. (2) If the obtaining of information for the determination of the content of a message is directed at a personal technical device that is suitable for sending and receiving a message and that is directly connected to a terminal end device, or it is directed at the connection between such personal technical device and a terminal end device, and the prerequisites provided in section 3 are fulfilled, the criminal investigation authority may be issued a warrant to obtain the information other than through telecommunications interception.
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	**The Criminal Code: Chapter 1 - Scope of application of the criminal law of Finland** *Section 1 - Offence committed in Finland* (1) Finnish law applies to an offence committed in Finland. (2) Application of Finnish law to an offence committed in Finland's economic zone is subject to the Act on the Economic Zone of Finland (1058/2004) and the Act on the Environmental Protection in Navigation (300/1979). *Section 2 - Offence connected with a Finnish vessel* (1) Finnish law applies to an offence committed on board a Finnish vessel or aircraft if the offence was committed

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	(1) while the vessel was on the high seas or in territory not belonging to any State or while the aircraft was in or over such territory, or (2) while the vessel was in the territory of a foreign State or the aircraft was in or over such territory and the offence was committed by the master of the vessel or aircraft, a member of its crew, a passenger or a person who otherwise was on board. (2) Finnish law also applies to an offence committed outside of Finland by the master of a Finnish vessel or aircraft or a member of its crew if, by the offence, the perpetrator has violated his or her special statutory duty as the master of the vessel or aircraft or a member of its crew. *Section 6 - Offence committed by a Finn* (1) Finnish law applies to an offence committed outside of Finland by a Finnish citizen. If the offence was committed in territory not belonging to any State, a precondition for the imposition of punishment is that, under Finnish law, the act is punishable by imprisonment for more than six months. (2) A person who was a Finnish citizen at the time of the offence or is a Finnish citizen at the beginning of the court proceedings is deemed to be a Finnish citizen. (3) The following are deemed equivalent to a Finnish citizen: (1) a person who was permanently resident in Finland at the time of the offence or is permanently resident in Finland at the beginning of the court proceedings, and (2) a person who was apprehended in Finland and who at the beginning of the court proceedings is a citizen of Denmark, Iceland, Norway or Sweden or at that time is permanently resident in one of those countries. *Section 8 - Other offence committed outside of Finland* Finnish law applies to an offence committed outside of Finland which, under Finnish law, may be punishable by imprisonment for more than six months, if the State in whose territory the offence was committed has requested that charges be brought in a Finnish court or that the offender be extradited because of the offence, but the extradition request has not been granted.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 10 - Place of commission (1) An offence is deemed to have been committed both where the criminal act was committed and where the consequence contained in the statutory definition of the offence became apparent. An offence of omission is deemed to have been committed both where the perpetrator should have acted and where the consequence contained in the statutory definition of the offence became apparent. (2) If the offence remains an attempt, it is deemed to have been committed also where, had the offence been completed, the consequence contained in the statutory definition of the offence either would probably have become apparent or would in the opinion of the perpetrator have become apparent. (3) An offence by an inciter and abettor is deemed to have been committed both where the act of complicity was committed and where the offence by the offender is deemed to have been committed. (4) If there is no certainty as to the place of commission, but there is justified reason to believe that the offence was committed in the territory of Finland, said offence is deemed to have been committed in Finland.
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	**The Extradition Act** *Section 2* Nationals of Finland shall not be extradited. *Section 4* (1)Extradition shall not be granted, unless the act referred to in the request is an offence or, if committed in Finland under corresponding circumstances, would constitute an offence the penalty for which may according to Finnish law be more severe than the deprivation of liberty for one year. --- (3)Where the request for extradition includes several acts and the prerequisites referred to above are fulfilled for any of them, extradition may be granted also for

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	the part of those other acts which, or the acts corresponding to, are punishable according to Finnish law. (4)Without prejudice to the provisions in paragraphs (1) and (2), extradition may be granted for an act which, if committed in Finland under corresponding circumstances, would constitute a counterfeiting offence, preparation of counterfeiting or the use of counterfeit money. **The Act on Extradition on the Basis of an Offence between Finland and other Member States of the European Union** *Section 2 – Extradition on the condition of dual criminality* (1) A request for extradition is granted if the act on which the request is based is punishable by the law of the requesting State by a custodial sentence of at least one year and the act, if committed in corresponding circumstances in Finland, is or would be an offence according to the law of Finland. … --- *Section 3 — Extradition without verification of double criminality* (1) Regardless of whether the act on which the request is based is an offence according to the law of Finland, the request for extradition shall be granted if according to the law of the requesting Member State the act is an offence referred to in paragraph 2 and the maximum penalty for the act provided by the law of said Member State is a custodial sentence for a maximum period of at least three years. Extradition for the enforcement of a custodial sentence further requires that the sanction imposed is a custodial sentence of at least four months. (2) The offences referred to above in paragraph 1 are: 1) participation in a criminal organisation; 2) terrorism; 3) trafficking in human beings; 4) sexual exploitation of children and child pornography; 5) illicit trafficking in narcotic drugs and psychotropic substances; 6) illicit trafficking in weapons, munitions and explosives; 7) bribery;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	8) fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention on the protection of the European Communities' financial interests (Treaty Series 85/2002); 9) laundering of the proceeds of crime; 10) counterfeiting currency, including of the euro; 11) computer network crime; 12) environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties; 13) facilitation of unauthorised entry and residence; 14) deliberate homicide, serious assault and serious causing of bodily injury; 15) illicit trade in human organs and tissue; 16) kidnapping, illegal restraint and hostage-taking; 17) racism and xenophobia; 18) organised and armed robbery; 19) illicit trafficking in cultural goods, including antiques and works of art; 20) swindling; 21) racketeering and extortion; 22) counterfeiting and piracy of products; 23) forgery of administrative documents and trafficking therein; 24) forgery of means of payment; 25) illicit trafficking in hormonal substances and other growth promoters; 26) illicit trafficking in nuclear or radioactive materials; 27) trafficking in stolen vehicles; 28) rape; 29) arson; 30) offences within the jurisdiction of the International Criminal Court; 31) unlawful seizure of aircraft and ships; 32) sabotage. *Section 4 — Accessory offences* If the request encompasses several acts and the prerequisites referred to in sections 2 or 3 are present for some acts, the request may be granted also in respect of those other acts that are or would be offences according to the law of Finland.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	The Criminal Code: Chapter 1 - Scope of application of the criminal law of Finland *Section 6 - Offence committed by a Finn* (1) Finnish law applies to an offence committed outside of Finland by a Finnish citizen. If the offence was committed in territory not belonging to any State, a precondition for the imposition of punishment is that, under Finnish law, the act is punishable by imprisonment for more than six months. (2) A person who was a Finnish citizen at the time of the offence or is a Finnish citizen at the beginning of the court proceedings is deemed to be a Finnish citizen. (3) The following are deemed equivalent to a Finnish citizen: (1) a person who was permanently resident in Finland at the time of the offence or is permanently resident in Finland at the beginning of the court proceedings, and (2) a person who was apprehended in Finland and who at the beginning of the court proceedings is a citizen of Denmark, Iceland, Norway or Sweden or at that time is permanently resident in one of those countries. *Section 8 - Other offence committed outside of Finland* Finnish law applies to an offence committed outside of Finland which, under Finnish law, may be punishable by imprisonment for more than six months, if the State in whose territory the offence was committed has requested that charges be brought in a Finnish court or that the offender be extradited because of the offence, but the extradition request has not been granted.
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.	**The Act on International Legal Assistance in Criminal Matters** *Section 1— Scope of application* (1) The provisions in this Act shall apply to international assistance in a criminal matter where the proceedings fall, at the time of the request for assistance, within the jurisdiction of a requesting Finnish authority or an authority of the requesting foreign State.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	(2) International assistance in criminal matters, as referred to in this Act, shall include: (1) service of decisions, summonses, notices and other judicial documents relating to a criminal matter, including summonses to appear before an authority of the requesting State; (2) hearing of witnesses, experts and parties, obtaining of expert opinions, inspections, procuring and transmitting documents and objects to be produced as as evidence, as well as the taking of any other evidence relating to a criminal matter; (3) search, seizure and the use of other coercive measures in order to obtain evidence or to secure the enforcement of a confiscation order; (4) institution of criminal proceedings; (5) communication of extracts from and information relating to judicial records required in a criminal matter; and (6) any other necessary assistance in a criminal matter, provision of information on law as well as any other forms of mutual co-operation. *Section 7— Form and content of requests* (1) A request for assistance transmitted by an authority of a foreign State to a Finnish authority may be made in writing, as a recording or orally; it may also be transmitted in an electronic message. Where the service of summons, notice, decision or other document is requested, the request shall be accompanied or supplemented by the document to be served. Where the authenticity of the request or any accompanying document is doubtful the Ministry of Justice or the competent authority may request for the necessary confirmation in writing. The request and the accompanying documents are exempt from legalisation or any similar formality. ----------
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	**The Act on International Legal Assistance in Criminal Matters** Section 27—*Secrecy, confidentiality and restrictions on the use of information*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(1) Where a Finnish authority makes a request for assistance to an authority of a foreign State, the provisions of Finnish law shall apply to the secrecy of documents and other records, confidentiality as well as to access to information by the parties and public authorities. (2) In addition to paragraph (1), the provisions in a treaty in force between Finland and the foreign State and the conditions set by the foreign State shall apply on secrecy, confidentiality, restrictions on the use of information and the return or destruction of the material provided by the requested State. **The Act on the Openness of Government Activities** *Section 30 — Granting access to secret information to the authority of a foreign state or to an international institution* In addition to the specific statutory provisions on the same, an authority may grant access to a secret official document to an authority of a foreign state or to an international institution, if an international agreement binding on Finland contains a provision on such co-operation between Finnish and foreign authorities, or there is a provision to this effect in an act binding on Finland, and if the Finnish authority in charge of the co-operation could under this Act have access to the document.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other;	**The Act on International Legal Assistance in Criminal Matters** *Section 3— Central authority* (1) The Ministry of Justice shall act as Central Authority and discharge the duties falling within the scope of application of this Act. --- *Section 4— Requests for assistance to Finnish authorities* (1) The request for assistance by an authority of a foreign State shall be transmitted to the Ministry of Justice or made directly to the authority competent to execute the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 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	(2) Where the request has been sent to the Ministry of Justice, the Ministry shall transmit it promptly to the authority competent to execute the request, unless the execution of the request falls within the competence of Ministry of Justice. *Section 9— Execution of requests* (1) The execution of the request shall be carried out in accordance with Finnish law, unless otherwise provided below. The request shall be executed promptly and the time limits set or implied in the request shall as far as possible be observed. (2) Where the request or the accompanying documents are defective to the extent that the request cannot be executed, the requesting authority of the foreign State shall be promptly requested to supplement the request or to provide additional information. (3) Where the request cannot be executed or the execution of the request is delayed, the authority of the requesting foreign State shall be promptly notified thereof and be informed of the reasons of the non-compliance or the delay. *Section 11—Compliance with a particular procedure specified in the request* (1) The request for assistance may be executed following a particular form or procedure specified in the request where such a form or procedure would not be incompatible with Finnish law. (2) Where the request cannot be executed in compliance with the procedure specified in the request, the authority of the requesting foreign State shall be promptly notified of the obstacles and inquired whether the request should nevertheless be executed. Section 12—*Mandatory grounds for refusal* (1) Assistance shall be refused, where the execution of the request would prejudice the sovereignty, the security or other essential interests of Finland.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) Assistance shall be refused, where the execution of the request would be contrary to the principles of human rights and fundamental freedoms or otherwise contrary to Finnish public policy (*ordre public*). Section 13—*Discretionary grounds for refusal* (1) Assistance may be refused, where: (1) the request relates to an offence that is of a political character or an offence under military law only; (2) the request relates to an offence, committed by a person who according to Finnish law could no longer be prosecuted by reason of lapse of time, pardon or by any other reason; (3) the request relates to an offence which in Finland or in a third State is subject to criminal investigations or under consideration of a prosecution authority or where court proceedings have been initiated; (4) the request relates to an offence for which the criminal investigations, prosecution or punishment, or any other punitive sanctions have been waived in Finland or in a third State; (5) the request relates to an offence in respect of which the offender has been sentenced or acquitted in Finland or in a third State; or (6) the execution of the request would, having regard to the nature of the offence, impose an unreasonable burden on the resources available. (2) The execution of the request may be postponed, if the execution of the request would cause inconvenience or delay in a criminal investigation, criminal investigations or court proceedings in Finland.
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:	**The Act on International Legal Assistance in Criminal Matters** Section 27—*Secrecy, confidentiality and restrictions on the use of information* (1) Where a Finnish authority makes a request for assistance to an authority of a foreign State, the provisions of Finnish law shall apply to the secrecy of documents and other records, confidentiality as well as to access to information by the parties and public authorities.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	(2) In addition to paragraph (1), the provisions in a treaty in force between Finland and the foreign State and the conditions set by the foreign State shall apply on secrecy, confidentiality, restrictions on the use of information and the return or destruction of the material provided by the requested State. --- On the legal assistance request of a foreign State documents including secret information may be delivered to be used as evidence if the delivery to a foreign State or the use as evidence is not prohibited by the law or restricted (Section 25 a(1); no translation available).
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	**The Act on International Legal Assistance in Criminal Matters** Section 23 - *Use of coercive measures to obtain evidence or to secure the enforcement of a confiscation order* (1) Search, seizure, data retention order, telecommunications interception, traffic data monitoring, the obtaining of information other than through telecommunications interception, obtaining location data in order to contact a suspect or convicted person, obtaining base station data, extended surveillance, covert collection of intelligence, technical surveillance, covert activity, pseudo-purchase, controlled delivery and taking of personal identifying characteristics in order to obtain evidence may be carried out pursuant to a request for assistance made by an authority of a foreign State, if this has been requested or deemed necessary in the execution of the request. --- Section 12—*Mandatory grounds for refusal* (1) Assistance shall be refused, where the execution of the request would prejudice the sovereignty, the security or other essential interests of Finland. (2) Assistance shall be refused, where the execution of the request would be contrary to the principles of human rights and fundamental freedoms or otherwise contrary to Finnish public policy (*ordre public*).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	Section 13—*Discretionary grounds for refusal* (1) Assistance may be refused, where: (1) the request relates to an offence that is of a political character or an offence under military law only; (2) the request relates to an offence, committed by a person who according to Finnish law could no longer be prosecuted by reason of lapse of time, pardon or by any other reason; (3) the request relates to an offence which in Finland or in a third State is subject to criminal investigations or under consideration of a prosecution authority or where court proceedings have been initiated; (4) the request relates to an offence for which the criminal investigations, prosecution or punishment, or any other punitive sanctions have been waived in Finland or in a third State; (5) the request relates to an offence in respect of which the offender has been sentenced or acquitted in Finland or in a third State; or (6) the execution of the request would, having regard to the nature of the offence, impose an unreasonable burden on the resources available. (2) The execution of the request may be postponed, if the execution of the request would cause inconvenience or delay in a criminal investigation, criminal investigations or court proceedings in Finland. *Section 15—Restrictions on coercive measures* (1) Where coercive measures are requested or where the request otherwise involves the use of coercive measures under the Coercive Measures Act (806/2011), such measures shall not be used, where not permitted under Finnish law had the offence to which the request relates been committed in Finland in similar circumstances. --- According to paragraph 2 (no translation available) the provision in paragraph 1 is not applicable to data retention order. Paragraphs 2, 6 and 7 are applicable as such without legislative provisions.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**The Act on International Legal Assistance in Criminal Matters** Section 23 - *Use of coercive measures to obtain evidence or to secure the enforcement of a confiscation order* (1) Search, seizure, data retention order, telecommunications interception, traffic data monitoring, the obtaining of information other than through telecommunications interception, obtaining location data in order to contact a suspect or convicted person, obtaining base station data, extended surveillance, covert collection of intelligence, technical surveillance, covert activity, pseudo-purchase, controlled delivery and taking of personal identifying characteristics in order to obtain evidence may be carried out pursuant to a request for assistance made by an authority of a foreign State, if this has been requested or deemed necessary in the execution of the request. --- Section 12—*Mandatory grounds for refusal* (1) Assistance shall be refused, where the execution of the request would prejudice the sovereignty, the security or other essential interests of Finland. (2) Assistance shall be refused, where the execution of the request would be contrary to the principles of human rights and fundamental freedoms or otherwise contrary to Finnish public policy (*ordre public*). Section 13—*Discretionary grounds for refusal* (1) Assistance may be refused, where: (1) the request relates to an offence that is of a political character or an offence under military law only; (2) the request relates to an offence, committed by a person who according to Finnish law could no longer be prosecuted by reason of lapse of time, pardon or by any other reason; (3) the request relates to an offence which in Finland or in a third State is subject to criminal investigations or under consideration of a prosecution authority or where court proceedings have been initiated;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) the request relates to an offence for which the criminal investigations, prosecution or punishment, or any other punitive sanctions have been waived in Finland or in a third State; (5) the request relates to an offence in respect of which the offender has been sentenced or acquitted in Finland or in a third State; or (6) the execution of the request would, having regard to the nature of the offence, impose an unreasonable burden on the resources available. (2) The execution of the request may be postponed, if the execution of the request would cause inconvenience or delay in a criminal investigation, criminal investigations or court proceedings in Finland.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	Section 23 - *Use of coercive measures to obtain evidence or to secure the enforcement of a confiscation order* (1) Search, seizure, data retention order, telecommunications interception, traffic data monitoring, the obtaining of information other than through telecommunications interception, obtaining location data in order to contact a suspect or convicted person, obtaining base station data, extended surveillance, covert collection of intelligence, technical surveillance, covert activity, pseudo-purchase, controlled delivery and taking of personal identifying characteristics in order to obtain evidence may be carried out pursuant to a request for assistance made by an authority of a foreign State, if this has been requested or deemed necessary in the execution of the request. --- **The Coercive Measures Act: Chapter 8 – Search** *Section 20 – Definition of a search of data contained in a device* (1) A *search of data contained in a device* refers to a search that is directed at the data that is contained at the time of the search in a computer, a terminal end device or in another corresponding technical device or information system. (2) A search of data contained in a device may not be directed at a confidential message, in respect of which Chapter 10 contains provisions on

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	telecommunications interception, traffic data monitoring and technical surveillance. *Section 21 – Prerequisites for a search of data contained in a device* (1) A search of data contained in a device may be conducted if: (1) there is reason to suspect that an offence has been committed and the most severe punishment provided for the offence is imprisonment for at least six months, or if the matter being investigated involves circumstances connected to the imposition of a corporate fine; and (2) it may be presumed that the search can lead to the discovery of a document or data to be seized as referred to in Chapter 7, section 1, subsections 1 or 2 or to a document to be copied on the basis of Chapter 7, section 2, and that is connected with the offence under investigation. (2) A search of data contained in a device may also be conducted in order to return the device to a person entitled to it, if there are grounds to suspect that it has been taken from someone by an offence. (3) The decision on the conduct of a search of the premises may be extended to cover also a technical device or information system in said premises, if the search in question is not one intended to find a person. **The Coercive Measures Act: Chapter 7 – Seizure and copying of a document** *Section 21 – Deciding on seizure on the basis of the request of a foreign state for mutual legal assistance* (1) An object, property, document or data may be seized at the request of a foreign authority if it may be used as evidence in a criminal case being considered by a foreign authority or if has been taken from someone through an offence. An object, property or document may be seized if, by a judgment of a court in a foreign state, it has been ordered forfeited on the basis of an offence or if it can justifiably be assumed that, in a case considered by a foreign state, the object shall be ordered forfeited on the basis of an offence. (2) The authority who decided on the seizure shall, within a week of the

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	decision, submit the decision on seizure for affirmation of the district court with jurisdiction over where the seizure was carried out. The court affirming the seizure shall at the same time establish the period of validity of the seizure. The court may, on the request of the authority who decided on the seizure, submitted before the end of the period of validity of seizure, decide to extend said period. Also the court considering the case and referred to in section 66, subsection 2 of the Act on Extradition on the Basis of an Offence Between Finland and Other Member States of the European Union (1286/2003) or section 63, subsection 2 of the Act on Extradition on the Basis of an Offence Between Finland and Other Nordic Countries (1383/2007) may decide on seizure. The prosecutor shall, when necessary, inform an authority that had earlier considered the question of seizure about the decision on seizure. (3) If an object, property or document has been seized to be used as evidence in a criminal case being considered by an authority of a foreign state, the court may decide, on the request of the authority that had decided on the seizure, that the object of the seizure may if necessary be transferred to the authority of the foreign state that had made the request, with the requirement that the object be returned after it is no longer needed as evidence in the case. The court may, however, order that the object, property or document need not be returned if return would clearly be inappropriate. (4) The provisions in sections 1–13, section 14, subsection 1, section 15, sections 17 and 22, section 23, subsections 3 and 4, and section 25 of this Chapter, in Chapter 3, section 1, subsection 2 and sections 5 and 6, as well as in the Act on Mutual Legal Assistance in Criminal Matters otherwise apply as appropriate to seizure in accordance with this section. The provisions in this Chapter on copies of documents may apply if this is possible in accordance with the request for mutual legal assistance or with the provisions on the granting of mutual legal assistance. (5) In lieu of subsections 1, 2 and 4, the provisions of the Act on Enforcement Within the European Union of Decisions From Other European Union Member States on the Freezing of Property or Evidence apply to enforcement of decisions on freezing referred to in said Act. In such a case, a criminal investigation authority or prosecutor may submit the request referred to in subsection 3 to the court.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) A request referred to in subsections 2 and 3 in respect of an order received from another Member State of the European Union for the surrender of evidence is submitted to the court referred to in section 10, subsection 2 of the Act on the National Enforcement and Application of the Framework Decision on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters (729/2010). Paragraphs 2 and 3 are applicable as such without legislative provisions.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	Article is applicable as such without legislative provisions.
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.	**The Act on International Legal Assistance in Criminal Matters** Section 23 - *Use of coercive measures to obtain evidence or to secure the enforcement of a confiscation order* (1) Search, seizure, data retention order, telecommunications interception, traffic data monitoring, the obtaining of information other than through telecommunications interception, obtaining location data in order to contact a suspect or convicted person, obtaining base station data, extended surveillance, covert collection of intelligence, technical surveillance, covert activity, pseudo-purchase, controlled delivery and taking of personal identifying characteristics in order to obtain evidence may be carried out pursuant to a request for assistance made by an authority of a foreign State, if this has been requested or deemed necessary in the execution of the request. ----------

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 15—Restrictions on coercive measures (1) Where coercive measures are requested or where the request otherwise involves the use of coercive measures under the Coercive Measures Act (806/2011), such measures shall not be used, where not permitted under Finnish law had the offence to which the request relates been committed in Finland in similar circumstances. ----------
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.	**The Act on International Legal Assistance in Criminal Matters** Section 23 - *Use of coercive measures to obtain evidence or to secure the enforcement of a confiscation order* (1) Search, seizure, data retention order, telecommunications interception, traffic data monitoring, the obtaining of information other than through telecommunications interception, obtaining location data in order to contact a suspect or convicted person, obtaining base station data, extended surveillance, covert collection of intelligence, technical surveillance, covert activity, pseudo-purchase, controlled delivery and taking of personal identifying characteristics in order to obtain evidence may be carried out pursuant to a request for assistance made by an authority of a foreign State, if this has been requested or deemed necessary in the execution of the request. ---------- *Section 15—Restrictions on coercive measures* (1) Where coercive measures are requested or where the request otherwise involves the use of coercive measures under the Coercive Measures Act (806/2011), such measures shall not be used, where not permitted under Finnish law had the offence to which the request relates been committed in Finland in similar circumstances. ----------
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	Pursuant to Article 35, paragraph 1, of the Convention, Finland has designated as the point of contact available on a twenty-four hour, seven-day-a-week basis the National Bureau of Investigation.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
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.	Pursuant to Article 14, paragraph 3.a, of the Convention, Finland has declared that it only applies Article 20 to offences aimed at a computer system committed by using telecommunications terminal equipment, pandering, threatening of persons to be heard in the administration of justice, menace, narcotic offences or attempts of the above, preparation of offences to be committed with terrorist intent and offences punishable by imprisonment of at least four years. Pursuant to Article 14, paragraph 3.b, of the Convention, the Finland has declared that it does not apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system if the system is being operated for the benefit of a closed group of users and does not employ public communications networks and is not connected with another computer system, whether public or private.

Back to the Table of Contents