Denmark

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 05 May 2020

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	Denmark did not copy verbatim into domestic law the four concepts defined in article 1. However, according to the preparatory works to act no. 352 of May 19 2004, Danish domestic law covers the four concepts in a manner consistent with the Convention.
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	Illegal access to information systems is criminalized in the following sections of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	the Criminal Code: - Section 263(2) regarding wrongfully (unjustifiable) gaining of access to any data or programs of another person intended for use in an information system. - Section 263a regarding wrongfully selling of or distribution to a wide group for commercial gain of a code or other means access to a non-public information system protected by a code or other special access protection and disclosure of a larger number of such codes or access means (concerns non-commercial systems). - Section 301a regarding wrongfully (unjustifiable) obtaining or disclosure of codes or other means of access to information systems where access is reserved for paying members and protected by a code or other special access restriction (concerns commercial systems). The (commercial) information systems in the Criminal Code Section 301a includes, inter alia, so-called on demand systems and information collections such as newspaper databases where access is reserved for paying members and protected by code, etc. The maximum penalty for violations of the Criminal Code Sections 263(2), 263a or 301a is 1 year and 6 months. However, if a person commits any act referred to in Section 263(2) with intent to obtain or become acquainted with the business secrets of an enterprise, or if other particularly aggravating circumstances apply, the penalty may increase to imprisonment for a term not exceeding 6 years. The same penalty is imposed for any of the offences referred to in subsection (2) which are committed in a systematic or organized manner. If any disclosure, etc., as referred to in the Criminal Code Section 263a is made in particularly aggravating circumstances, under subsection (4) the penalty is

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	imprisonment for a term not exceeding 6 years. Especially situations where information is disclosed or otherwise imparted to a very considerable extent, or the disclosure entails a particular risk of serious harm, are considered particularly aggravating circumstances. If any disclosure, etc., as referred to in the Criminal Code Section 301a is made in particularly aggravating circumstances, under subsection (2) the penalty is imprisonment for a term not exceeding 6 years. Especially situations where information is disclosed or otherwise imparted for commercial gain to a large group of people or in circumstances entailing a particular risk of serious abuse are considered particularly aggravating circumstances.
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.	Illegal interception of computer data is criminalized in the Criminal Code Section 263(2) regarding wrongfully (unjustifiable) gaining of access to any data or programs of another person intended for use in an information system. Reference is made to the comments about Section 263(2) under illegal access to information (see under article 5).
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.	Reference is made to the comments regarding article 5, since deletion, damaging, etc., of computer data is criminalized by the same Sections of the Criminal Code as the Sections mentioned regarding article 5 and illegal system interference.
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	Illegal system interference is criminalized in the following sections of the Criminal Code: - Section 193(1) regarding the causing of comprehensive interference with the operation of any public transport means, public postal service,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	telegraph or telephone service, radio or television broadcasting system, information system or service providing public utility supplies of water, gas, electricity or heating. - Section 291(1) regarding destroying, damaging or removal of any property belonging to another person. - Section 293(2) regarding wrongfully preventing another person from disposing of an item in full or in part. Deleting, damaging, deteriorating, altering or suppressing computer data is covered by Section 291 of the Criminal Code. Denial of service attacks that prevents the normal use of or access to data systems by overload or by causing a break down is criminalized under Section 293(2). The term comprehensive interference in the Criminal Code Section 193 is used for acts that have potential to affect the general public in terms of information systems, etc. An example of such act is the deletion of an internet provider's data system or other hacking causing interference with a critical infrastructure information system. The maximum penalty for violations of the Criminal Code Section 193 is 6 years, while the maximum penalty for violations of Section 293(2) is 1 year. However, the sentence under Section 293(2) may increase to imprisonment for 2 years if an offence is committed in a systematic or organized manner or in otherwise particularly aggravating circumstances. The maximum penalty for violations of the Criminal Code Section 291(1) is 1 year and 6 months. In case of serious criminal damage or criminal damage in a systematic or organized manner, or if the offender has previously been convicted under this section 291 or under section 180, section 181, section 183(1) and (2), section 184(1), section 193 or section 194, the sentence may

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	increase to imprisonment for 6 years.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	Production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools is not criminalized per se. However, the production, procurement etc. of devices or tools with features that can be misused for the use in criminal offences is punishable as incitement or aiding and abetting to an offence (Section 23) or attempting to commit an offence (Section 21). Hence, planning to design a program with the intention to use it in a cyber attack is punishable as an attempt to commit, inter alia, illegal interference according to section 293(2).
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	Computer-related forgery is criminalized in Section 171 regarding fraud. The section applies to forgery of electronic data. Hence, the offence covers every

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	electronic data that form a verification, including e-mails, voice-mails etc. The maximum penalty for violations of Section 171 is 2 years of imprisonment. If the forgery is particularly aggravating or multiple offences of the same sort has been made the penalty may increase to imprisonment for a term not exceeding 6 years.
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.	Computer-related fraud is criminalized in the Danish Criminal Code Section 279a regarding data fraud. To secure criminalization of cases of fraud where no human person is misled because the treatment of information/data is made by an information system, this section was introduced in 1985. The maximum penalty for violations of Section 279a is imprisonment for 1 year and 6 months. However, if the data fraud is of a particularly aggravating nature, especially because of the methods used, because the offence was committed jointly by several or due to the scope of the gain made or intended, or when several offences has been committed, the penalty may increase to imprisonment for a term not exceeding 8 years Section 286(2).
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a	Computer-related production of child pornography involving a child below the sexual age of consent is criminalized in the following sections of the Criminal Code: - Section 216(2) regarding sexual intercourse with a child below 12 years of age (Section 225 if the sexual act concerns other sexual activity than intercourse) - Section 222 sexual intercourse with a child below the age of sexual consent (Section 225 if the sexual act concerns other sexual activity

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	than intercourse) - Section 226 regarding production of pornographic photographs, pornographic films or similar recordings of a person under 18 years of age with intent to sell or otherwise distribute the material - Section 232 regarding indecency Computer-related production of child pornography involving a child above the age of sexual consent is criminalized in the following sections of the Criminal Code: - Section 226 regarding production of pornographic photographs, pornographic films or similar recordings of a person under 18 years of age with intent to sell or otherwise distribute the material - Section 232 regarding indecency Production of computer generated child pornographic images is criminalized in the following sections of the Criminal Code: - Section 235(2) regarding possession or view, for value or through the Internet or a similar system for dissemination of information, of pornographic photographs or films or other pornographic visual reproductions or similar recordings of persons under 18 years of age - Section 226 regarding production of pornographic photographs, pornographic films or similar recordings of a person under 18 years of age with intent to sell or otherwise distribute the material Computer-related distribution of child pornography is criminalized in Section

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	235(1) of the Criminal Code regarding distribution of pornographic photographs or films or other pornographic visual reproductions or similar recordings of persons below 18 years of age. Computer-related possession of child pornography is criminalized in Section 235(2) of the Criminal Code regarding possession or view, for value or through the Internet or a similar system for dissemination of information, of pornographic photographs or films or other pornographic visual reproductions or similar recordings of persons under 18 years of age. However, it follows from Section 235(3) of the Danish Criminal Code that possession of material involving a child who has reached the age of sexual consent with the consent of that child falls outside the scope of Section 235(2). The term pornographic photographs, pornographic films or similar recordings of persons below 18 years of age includes persons appearing to be a child. However, if the depicted person appearing to be a child was in fact 18 years of age or older at the time of depiction the material is not considered as child pornography. The term pornographic visual reproductions or similar recordings of persons under 18 years of age means in particular computer generated images that do not depict a real person under 18 years, but apart from the fictional aspect have a full resemblance with a photograph. The fictional production must therefore appear in approximately the same way as photographs and the like. Criminal liability for the abovementioned offences require intend (Section 19, cf. Sections 216(2), 222, 226, 232 and 235 of the Criminal Code). However, pursuant to Section 228 of the Criminal Code criminal liability for violations of Sections 222 and 226 can be incurred despite lack of knowledge of the victim's age if the perpetrator acted negligently with respect to the victim's age. The maximum penalty for violations of Sections 216(2) of the Criminal Code is 12 years. The maximum penalty for violations of Section 222 is imprisonment for a term not exceeding 8 years. If the perpetrator has used coercion or threats the maximum penalty is imprisonment for a term not exceeding 12 years. The maximum penalty for violations of Section 226 is imprisonment for a term not

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	exceeding 6 years. The maximum penalty for violations of Section 232 is imprisonment for a term not exceeding 4 years if the child is below 15 years and imprisonment for a term not exceeding 2 years if the child is 15 years or older. The maximum penalty for violations of Section 235(1) is imprisonment for a term not exceeding 2 years or in particularly aggravating circumstances imprisonment for a term not exceeding six years. The maximum penalty for violations of Section 235(2) is imprisonment for a term not exceeding 1 year. Computer-related "grooming" is criminalized as an attempt (Section 21) to commit a sexual offence against a child pursuant to Chapter 24 of the Criminal Code, e.g. an attempt to engage in sexual intercourse with a child who has not reached the legal age for consent or to produce child pornography. Because "grooming" is criminalized as an attempt to commit a sexual offence "grooming" is not defined in the Criminal Code. However, criminal liability for attempt includes in principle any preparatory action irrespective of whether the action itself is harmless or unsuitable as a mean to commit the intended crime. Thus, computer-related "grooming" may be punishable from the time the perpetrator first contacts the child with the intent to commit the sexual offence regardless of whether the contact is initiated by means of information and communication technology or whether the perpetrator has proposed to meet the child and taken material acts leading to such a meeting. The maximum penalty for computer-related "grooming" relates to the offence that the perpetrator attempted to commit. E.g. the maximum penalty for computer-related "grooming" with an intend to produce child pornography intended for distribution (Section 21 and Section 226) of the Criminal Code, is the maximum penalty for production of child pornography with the intend to distribute the material which is imprisonment for a term not exceeding 6 years.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	Reference is made to section 299 b of the Criminal Code which states:

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 the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	"Section 299 b. (1) Imprisonment for a term not exceeding six years is imposed on any person who, to obtain an unlawful gain for himself or others or in otherwise aggravating circumstances, is guilty of - 1. (i)particularly aggravating copyright infringements as set out in section 76(2) of the Copyright Act (ophavsretsloven) or particularly aggravating illegal imports as set out in section 77(2) of the Copyright Act; 2. (ii)particularly aggravating trademark infringements as set out in section 42(2) of the Trademark Act (varemærkeloven); 3. (iii)particularly aggravating design right infringements as set out in section 36(2) of the Design Act (designloven); 4. (iv)particularly aggravating patent right infringements as set out in section 57(2) of the Patent Act (patentloven); 5. (v)particularly aggravating utility model infringements as set out in section 54(2) of the Utility Model Act (brugsmodelloven); 6. (vi)particularly aggravating violation of section 91, cf. section 94(2), of the Act on Radio and Television Broadcasting (lov om radio- og fjernsynsvirksomhed)." Furthermore, reference is made to sections 76 and 77 of the Consolidated Act on Copyright which states: "Section 76**.** Anyone who with intent or by gross negligence i. violates section 2 or section 3, ii. violates sections 65, 66, 67, 69, 70 or 71, iii. violates section 11 (2), section 60 or sections 72-75, iv. fails to file a statement or information according to section 38 (7), v. fails to register or fails to disclose information to the joint organisation according to section 41 (1), section 42 (6) and the first sentence of section 46, or fails to keep and hold accounts according to section 45, or vi. violates regulations laid down pursuant to section 61 (2) is liable to a fine. (2) Where an intentional violation of the provisions mentioned in subsection (1) (i) and (ii) has been committed by using works, performances or productions

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	protected under sections 65-71 or by distributing copies hereof among the general public, the punishment may under particularly aggravating circumstances be increased to imprisonment in one year and 6 months, unless a more severe punishment is provided by section 299 b of the Criminal Code. Particularly aggravating circumstances are deemed to exist especially where the offence is commercial, concerns production or distribution of a considerable number of copies, or where works, performances or productions are made available to the public in such a way that members of the public may access them from a place and at a time individually chosen by them, cf. the second division of section 2 (4) (i). Section 77. Where copies of works or of performances or productions that are protected under sections 65-71 have been produced outside Denmark under such circumstances that a similar production in Denmark would have been in conflict with the law, anyone who with intent or by gross negligence imports such copies with a view to making them available to the public shall be liable to a fine. (2) The provision of section 76 (2) shall apply correspondingly to intentional violations of the provision of subsection (1).”
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.	Reference is made to sections 21 and 23 of the Criminal Code which states: *“Section 21.* Acts aimed at inciting or assisting the commission of an offence are punishable as attempts if the offence is not completed. (2) The penalty prescribed for an offence may be reduced for attempts, especially where an attempt reflects little strength or persistence of criminal intent. (3) Unless otherwise provided, attempts will only be punished if the offence is punishable by imprisonment for a term exceeding four months.”

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	"*Section 23.* The penalty provided for an offence applies to everybody who is complicit in the act by incitement or aiding and abetting. The punishment may be reduced where a person intended only to provide minor assistance or support an intent already formed, and where the offence has not been completed or intentional complicity failed. (2) The punishment may also be reduced where a person is complicit in the breach of a special duty to which he is not subject. (3) Unless otherwise provided, the punishment for complicity in offences that do not carry a sentence of imprisonment for a term exceeding four months may be remitted where the accomplice intended only to provide minor assistance or support an intent already formed, and where his complicity was due to negligence."
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.	Legal persons are liable for the crimes that are referred in the abovementioned sections of the Criminal Code and the Consolidated Act on Copyright. Thus, reference is made to section 306 of the Criminal Code which states: "*Section 306.* Companies and other incorporated bodies (legal persons) may incur criminal liability under the rules of Part 5 [section 25-27] for violation of this Code." Reference is made to sections 25-27 of the Criminal Code which states: "*Section 25.* A fine may be imposed on a legal person where so provided by or pursuant to statute. *Section 26.* Provisions on the criminal liability of companies and other corporations comprise any legal person, including public and private limited companies, cooperative societies, partnerships, associations, societies, foundations, estates and local and state authorities, unless otherwise provided. (2) Those provisions also comprise sole proprietorships if they are comparable to the enterprises referred to in subsection (1), especially in view of their size

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and organisation. *Section 27.* It is a condition precedent to the criminal liability of a legal person that an offence has been committed in the course of its activities and that the offence was caused by one or more natural persons connected to the legal person or by the legal person as such. Section 21 (3) on punishment for attempts applies correspondingly. (2) State and local authorities may only be punished for offences committed in carrying on activities which are equal or comparable to activities carried on by private individuals.”
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	Reference is made to the comments regarding article 2-12.
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.	Reference is made to the comments regarding article 16-21.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.	Reference is made to the comments regarding article 16-21.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Expedited preservation of stored computer data and traffic data, as well as partial disclosure of traffic data, is regulated by Sections 786 a and 804 of the Administration of Justice Act: **"The Administration of Justice Act Section 786 a.** **(1)** In connection with an investigation in which electronic evidence may be of importance, the police may impose orders on providers of telecom networks or services to arrange for emergency protection of electronic data, including traffic data. **(2)** An order of emergency protection under subsection (1) above may solely comprise electronic data stored at the point in time when the order is imposed. The order must state the data that must be secured and the period for which they must be secured (the period of protection). The order must be limited to comprise solely the data estimated to be necessary for investigation and the protection period must be as short as possible and no more than 90 days. An order of this nature may not be extended. **(3)** Providers of telecom networks or services are responsible for ensuring as part of the protection under subsection (1) without undue delay that they pass on traffic data concerning other telecom network or service providers whose networks or services have been used in connection with the electronic communication that may be of importance for the investigation. **(4)** Violation of subsections (1) and (3) above is punishable by a fine." **"The Administration of Justice Act Section 804.** **(1)** In connection with the investigation of an offence which is subject to public prosecution or a case of violation of an order as referred to in section 2(1) para. 1 of the Act on Restraining, Exclusion and Removal Orders, a person who is not a suspect may be ordered to produce or hand over objects (discovery), if there is reason to presume that an object of which that person has the disposal may serve as evidence, should be confiscated or, by the offence, has been procured from someone who is entitled to claim it back. When an order is imposed on a

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	business enterprise, section 189 shall apply correspondingly to others who have gained insight into the case due to their association with the enterprise. **(2)** If an object has been handed over to the police following an order of discovery, the rules of seizure according to section 803(1) shall apply correspondingly. **(3)** If, without any order to this effect, an object has been handed over to the police for the reasons mentioned in subsection (1) above, section 807(5) shall apply. If a request for return of an object is made, and the police do not grant the request, the police shall as soon as possible and within 24 hours submit the case to the court with a request for a seizure order. In that case section 806(4), 2nd sentence, and subsection (6) 1st sentence, shall apply. **(4)** An order of discovery may not be issued if it will produce information on matters about which the individual would be exempted from testifying as a witness according to sections 169-172. **(5)** The Minister of Justice may issue rules on financial compensation in special cases for costs relating to the fulfilment of an order for discovery." Sections 786 a and 804 of the Administration of Justice Act cover all kinds of electronic data and apply to electronic evidence in relation to any criminal offence.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.	Reference is made to the comments under article 16.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
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.	Reference is made to the comments made under article 16 regarding Section 804. **"The Administration of Justice Act Section 804.** **(1)** In connection with the investigation of an offence which is subject to public prosecution or a case of violation of an order as referred to in section 2(1) para. 1 of the Act on Restraining, Exclusion and Removal Orders, a person who is not a suspect may be ordered to produce or hand over objects (discovery), if there is reason to presume that an object of which that person has the disposal may serve as evidence, should be confiscated or, by the offence, has been procured from someone who is entitled to claim it back. When an order is imposed on a business enterprise, section 189 shall apply correspondingly to others who have gained insight into the case due to their association with the enterprise. **(2)** If an object has been handed over to the police following an order of discovery, the rules of seizure according to section 803(1) shall apply correspondingly. **(3)** If, without any order to this effect, an object has been handed over to the police for the reasons mentioned in subsection (1) above, section 807(5) shall apply. If a request for return of an object is made, and the police do not grant the request, the police shall as soon as possible and within 24 hours submit the case to the court with a request for a seizure order. In that case section 806(4), 2nd sentence, and subsection (6) 1st sentence, shall apply. **(4)** An order of discovery may not be issued if it will produce information on matters about which the individual would be exempted from testifying as a witness according to sections 169-172. **(5)** The Minister of Justice may issue rules on financial compensation in special cases for costs relating to the fulfilment of an order for discovery."
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:	Search and seizure of information is possible during investigation of an offence in relation to cybercrime according to Chapter 73 and 74 of The Administration of Justice Act. Sections 793 to 807 contain general provisions on trace, search,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 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.	seizure and freezing. Section 793 sets out the scope of application of the rules on search. Investigations of all the offences mentioned under article 2-10 can be grant access to a search on the conditions that there are reasonable grounds to suspect the person whose property is subject to the search of committing the crime and on condition that the search presumably is of substantial importance to the investigation. Search of a third party's (non-suspects') property can be made when there is reason to presume that evidence or items subject to seizure can be found. Rules on the need for a court order on search and the general conditions for a search are found in Section 796 to 798. Section 801 lays down the general scope of application of the provisions on seizure and defines the purposes of seizure. The most ordinary causes for seizure according to Section 802 are reason to presume that the items can serve as evidence or should be confiscated on the basis of reasonable grounds to suspect the owner or the holder. Seizure can also be made of a third party's items and property on the same conditions as from a suspect.
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	Reference is made to the comments made under article 21.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified	The use of real-time interception of traffic and content data according to Section 791 b is restricted to the serious cybercrime offences punishable with six years of imprisonment. Hence, interception is not possible as part of a investigation of illegal hindering of dispositions of computer data etc., e.g. a denial of service attack, according to Section 293(2) of Criminal Code. In addition to this basic condition, reasonable grounds to presume that information's are used or being passed from a suspect need to be present as well as a presumption that the interception is of essential importance to the investigation. Interception of telecommunications (content data) etc. is also available according to Section 781 to the serious cybercrime offences punishable with at least six years of imprisonment if there are reasonable grounds to presume that information is used or being passed from a suspect and that the interception is presumed to be of essential importance to the investigation. This measure includes disclosure of email-correspondence and other available content. This Section concerns tapping communication through the service provider's

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	facilities, in contrast to interception under Section 791b that covers "skimming" of computer (or other information system).
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	The Danish jurisdiction rules in Sections 6-9 in the Criminal Code provide for jurisdiction with regard to, inter alia, cybercrime acts committed partially or entirely outside Denmark. Section 6 of the Criminal Code provides: "Acts falling within Danish criminal jurisdiction are acts committed – (i) within the Danish state; (ii) on board a Danish vessel or aircraft located within the territory of another state by a person belonging to or travelling on the vessel or aircraft; or (iii) on board a Danish vessel or aircraft located outside the territory of any state." Reference is made to Section 9(2) of the Criminal Code. In Section 9 it is stated: "(1) Acts are deemed to have been committed at the place where the offender was when the act was committed. As regards legal persons, acts are deemed to have been committed at the place where the act(s) implying the liability of the relevant legal person were committed.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) If the criminality of an act depends on or is influenced by an actual or intended consequence, the act is also deemed to have been committed at the place where the effect occurred, or where the offender intended the effect to occur. (3) Attempts or acts of complicity are deemed to have been committed within the Danish state if the offender was in Denmark when the act was committed, irrespective of whether the offence was completed or intended to be completed outside the Danish state. (4) Where part of an offence was committed within the Danish state, the full offence is deemed to have been committed in Denmark." Section 7 of the Criminal Code concerns the active personality principle. Section 7 states: "(1) Acts committed within the territory of another state by a person who was a Danish national or has his abode or similar habitual residence within the Danish state at the date of the provisional charge are subject to Danish criminal jurisdiction, if – (i) the act is also a criminal offence under the legislation of the country in which the act was committed (dual criminality); or (ii) the offender had the aforesaid attachment to Denmark when committing the act and such act -(a)comprises sexual abuse of children, human trafficking or female circumcision; or (b)is aimed at someone having the aforesaid attachment to Denmark when the act was committed. (2) Acts committed outside the territory of any state by a person having such attachment to Denmark as referred to in subsection (1) at the date of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	provisional charge are also subject to Danish criminal jurisdiction, provided that acts of the kind described may carry a sentence of imprisonment for a term exceeding four months. (3) Subsections (1)(i) and (2) apply, with the necessary modifications, to acts committed by a person who is a national of or has his abode in Finland, Iceland, Norway or Sweden at the date of the provisional charge, and who is staying in Denmark." With regards to the passive personality principle reference is made to Section 7a of the Criminal Code. In Section 7a it is stated: "(1) Acts committed within the territory of another state and aimed at a person who was a Danish national or had his abode or similar habitual residence within the Danish state when the act was committed are subject to Danish criminal jurisdiction if any such act is also a criminal offence under the legislation of the country in which the act was committed (dual criminality) and may carry a sentence under Danish legislation of imprisonment for at least six years. (2) Danish criminal jurisdiction under subsection (1) only applies to the acts of – (i) murder; (ii) aggravated assault, deprivation of liberty or robbery; (iii) offences likely to endanger life or cause serious injury to property; (iv) sexual offences or incest; or (v) female circumcision. (3) Acts committed outside the territory of any state, but aimed at someone having such attachment to Denmark as referred to in subsection (1) when the act was committed are also subject to Danish criminal jurisdiction, provided that acts of the kind described may carry a sentence of imprisonment for a term

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	exceeding four months." Regarding legal persons reference is made to Section 7b of the Criminal Code: "Where the application of Danish criminal jurisdiction to a legal person is subject to dual criminality, the criminal liability of legal persons need not be prescribed by the legislation of the country in which the act was committed."
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds	The question of extradition is determined pursuant to the Consolidated Act of 25 August 2005, No. 833, with later amendments, on Extradition of Offenders (the Extradition Act). Extradition is not conditional upon the existence of a treaty. Extradition is thus possible also where no agreement on extradition has been made between Denmark and the relevant foreign country. Extradition of non-Danish nationals to countries outside the EU under the Extradition Act can take place if the offence is punishable under Danish law with imprisonment of one year or more, cf. Section 2 a. This requirement is satisfied in cases concerning cybercrime, i.e. the acts mentioned in article 2-11. If the extradition concerns enforcement of a judgment, the person must have been sentenced to four months imprisonment or more in the requesting country or have been committed to a mental institution for a minimum of four months, cf. Section 3. A Danish national can be extradited to countries for criminal prosecution outside the EU if, for the last two years prior to the criminal act, he has had his residence in the country to which extradition is desired, and an act corresponding to the offence for which extradition is sought carries a maximum penalty of at least one year according to Danish law, or the criminal act may entail a more severe penalty than imprisonment for 4 years under Danish law, cf. Section 2(1). The extradition must normally be based on an agreement with the other country, but if there is no such agreement the Minister of Justice (Since 1 June 2016, the Director of Public Prosecutions, cf. below) may, anyhow, decide to extradite a Danish national based on the same requirements,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	cf. Section 2(2). Danish nationals are not extradited for enforcement to countries outside the EU and Nordic countries. Special provisions apply within the EU in order for Denmark to comply with the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant ("the Framework Decision"). The provisions in the Extradition Act concerning extradition from Denmark to another EU Member State on a European arrest warrant differ in several ways, e.g.: • Dual criminality is not required in the case of extradition for a large number of offences, specified in the "positive list", including child pornography and computer-related crime (Extradition Act, art. 10 a, no. 4 and 11). • Danish nationals are basically extraditable in the same way as foreign nationals. • Extradition is not refusable on the grounds that the offences involved are political or that there is insufficient evidence to support the charge or conviction for an act for which extradition is sought. • The issuing of a European arrest warrant will in itself provide the basis on which to secure a person's arrest and extradition for prosecution or service of sentence. • A European arrest warrant has to be dealt with within short time limits and the Act includes deadlines for processing a decision on extradition and for any judicial review of that decision. Furthermore, special provisions apply with regard to extradition to Nordic countries (Finland, Iceland, Norway and Sweden). Extradition from Denmark to Nordic countries for the purpose of criminal prosecution or execution of a sentence can take place on basis of a Nordic arrest warrant, cf, Section 10 k. A Nordic arrest warrant can be issued if the charge for which extradition is sought is punishable with imprisonment or any other measure involving deprivation of liberty. Extradition for the purpose of execution of a sentence can take place if the person in question has been sentenced to imprisonment or any other measure involving deprivation of liberty.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Denmark has criminal jurisdiction over Danish nationals who have committed criminal offences abroad subject to certain conditions, cf. Sections 7 and 8 of the Criminal Code. E.g. Danish nationals whose extradition is declined with reference to their nationality can thus be prosecuted in Denmark. When prosecution takes place in Denmark under the provisions above, the decision both concerning the punishment and any other legal consequences of the act must be made under Danish law, cf. Section 10 (1) of the Criminal Code. In the circumstances where the act is subject to Danish criminal jurisdiction pursuant to Section 7 of the Criminal Code, the punishment may not be more severe than that provided for by the law of the territory where the act was committed, cf. Section 10 (2) of the Criminal Code. It depends on a recommendation from the prosecutor whether a request for transfer of proceedings should be made to another country. One guideline for the prosecutor's decision thereon will be where the proceedings can be conducted most conveniently. Transfer of proceedings is made on the basis of the rules in the European Convention on the Transfer of Proceedings in Criminal Matters. As a point of departure, transfer is only possible in relation to countries that have acceded to the Transfer Convention. Pursuant to Section 5 of the Act on Transfer of Proceedings, the Minister of Justice may, however, decide on the basis of mutuality that the Act must also be applied in the relationship between Denmark and a country that has not acceded to the Convention. Pursuant to Section 8 of the Criminal Code, depending on the circumstances, Denmark has criminal jurisdiction in relation to acts committed abroad, irrespective of the nationality of the perpetrator. This applies, inter alia, in cases where the act is covered by an international convention in pursuance of which Denmark is under an obligation to start legal proceedings, cf. Section 8, no. 5. One of the purposes of this provision is to satisfy and make possible the compliance with future conventions or other international covenants involving an obligation for Denmark to have Danish criminal jurisdiction so as to be able to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	prosecute specified offences. The Director of Public Prosecutions has since 1 June 2016 been designated as the central authority for extradition requests from and to States outside the Nordic countries (Finland, Iceland, Norway and Sweden), whereas requests from and to the Nordic countries are sent to and received by the relevant police district. Until 1 June 2016, the Ministry of Justice was designated as central authority.
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested 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	There is no specific Danish legislation relating to mutual legal assistance in criminal matters. In all cases where assistance from Denmark is required, the Danish authorities apply national legislation by analogy. This implies that Danish authorities can comply with requests for mutual legal assistance even though no bilateral or multilateral agreement exists between Denmark and the requesting country. This also implies that Danish authorities can comply with a request if the investigative measure(s) covered by the request could be carried out in a similar national case. Therefore, requests are executed in accordance with national law concerning criminal procedure (The Administration of Justice Act) and - if applicable - in accordance with relevant international instruments such as the 1959 Council of Europe Convention on Mutual Legal Assistance and Agreements between the Nordic countries. Danish law enforcement authorities can always provide foreign law enforcement authorities with requested information. In some cases, there can be a restriction on the further use of the information, for example if there is an on-going investigation in Denmark. The Ministry of Justice was until 1 March 2016 designated as central authority to receive requests for mutual legal assistance and to execute them or in some cases transmit them to the competent authorities for execution. Requests are executed where appropriate by one or more authorities, e.g. the Danish State Prosecutor for Serious Economic and International Crime, the Police or the Prosecution Service. Since 1 March 2016, the Director of Public Prosecutions has been designated as

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	central authority instead of the Ministry of Justice. In general, requests for mutual legal assistance and any communication related thereto must be transmitted to the Director of Public Prosecutions by the requesting State. However, urgent requests and communications may be addressed through diplomatic channels, Europol, Interpol or directly to the relevant authorities. Additionally, any requests sent within the Schengen system or requests on the basis of the European Convention of 29 May 2000 on Mutual Assistance in Criminal Matters may be sent directly to the relevant judicial authorities. Requests may be sent by e-mail or by regular mail. Denmark has no special limitations concerning fiscal matters. Thus, Denmark does not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters. It can be noted in this connection that the 1978 Additional Protocol to the Council of Europe Convention on Mutual Assistance in Criminal Matters withdraws the possibility of refusing assistance solely on the ground that the request concerns an offence which the requested party considers a fiscal offence. There are only a few areas where information due to secrecy provisions (legal professional privileges etc.) is not available in an investigation, for example obtaining information exchanged between a suspect and his defense attorney. Assistance is always given unless it is impossible. In a few cases, assistance which requires dual criminality, is denied because there is no such duality but in such situations it will be discussed with the requesting country whether they can provide additional information which might enable the Danish authorities to comply with the request or if more limited assistance not involving coercive measures is wanted. Dual criminality is not required for non coercive measures. In the Danish legal system, dual criminality is seen as a question of whether the same facts are criminalized and not as formal duality. This implies that dual

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	criminality is considered on the basis of the underlying conduct rather than on the basis of specific offences.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	Law enforcement authorities can in accordance with Danish law exchange information with foreign counterparts for intelligence or investigative purposes. There are no special restrictions to the exchange of information between law enforcement authorities provided that the exchange is necessary to fight crime and that the secrecy and data protection provisions in the receiving country are found to be sufficient.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep	Reference is made to the comments above under article 25.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	Reference is made to the comments above under article 25.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the	As mentioned above under the comments to article 25, there is no specific Danish legislation concerning mutual legal assistance in criminal matters. In all

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure	cases where mutual legal assistance from Denmark is required the Danish authorities apply national legislation by analogy. This implies that the Danish authorities can comply with a request for mutual legal assistance if the investigative measures covered by the request could be carried out in a similar national case. With regard to foreign requests for expedited preservation of stored computer data, reference is therefore made to the comments above to article 16, cf. article 25.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	As mentioned above under the comments to article 25, there is no specific Danish legislation concerning mutual legal assistance in criminal matters. In all cases where mutual legal assistance from Denmark is required the Danish authorities apply national legislation by analogy. This implies that the Danish authorities can comply with a request for mutual legal assistance if the investigative measures covered by the request could be carried out in a similar national case. With regard to foreign requests for expedited disclosure of preserved traffic data, reference is therefore made to the comments to article 17, cf. article 25.
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	As mentioned above under the comments to article 25, there is no specific Danish legislation concerning mutual legal assistance in criminal matters. In all cases where mutual legal assistance from Denmark is required the Danish authorities apply national legislation by analogy. This implies that the Danish authorities can comply with a request for mutual legal assistance if the investigative measures covered by the request could be carried out in a similar national case. With regard to foreign requests for search and seizure of stored computer data, reference is therefore made to the comments to article 19, cf. article 25.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 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.	As mentioned above under the comments to article 25, there is no specific Danish legislation concerning mutual legal assistance in criminal matters. In all cases where mutual legal assistance from Denmark is required the Danish authorities apply national legislation by analogy. This implies that the Danish authorities can comply with a request for mutual legal assistance if the investigative measures covered by the request could be carried out in a similar national case. With regard to foreign requests for real-time collection of traffic data, reference is therefore made to the comments to article 20, cf. article 25.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall	**Declaration contained in a letter from the Permanent Representative of Denmark, dated 28 September 2005, registered at the Secretariat General on 30 September 2005 – Or. Engl.** In accordance with Article 35, paragraph 1, of the Convention, the Government of the Kingdom of Denmark has designated as competent authority:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	The Danish National Police Police Department Polititorvet 14, DK-1780 Copenhagen V Denmark
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.	**Reservation contained in the instrument of ratification deposited on 21 June 2005 - Or. Engl.** In accordance with Article 9, paragraph 4, of the Convention, the Government of the Kingdom of Denmark declares that the criminal area according to Article 9 shall not comprehend the possession of obscene pictures of a person attained the age of fifteen, if the person concerned has given his or her consent to the possession, cf. Article 9, paragraph 1, letter e. **Period covered: 01/10/2005 -** Articles concerned : 9 **Reservation contained in the instrument of ratification deposited on 21 June 2005 - Or. Engl.** In accordance with Article 9, paragraph 4, of the Convention, the Government of the Kingdom of Denmark declares that the criminal area according to Article 9 shall not comprehend visual representations of a person appearing to be a minor engaged in sexually explicit conduct, cf. Article 9, paragraph 2, letter b.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Period covered: 01/10/2005 - Articles concerned : 9 **Reservation contained in the instrument of ratification deposited on 21 June 2005 - Or. Engl.** In accordance with Article 14, paragraph 3, letter a,of the Convention, the Government of the Kingdom of Denmark declares that Denmark will only apply article 20 concerning monitoring of traffic data to the extent where in accordance with Article 21 there is an obligation to empower the competent authorities to monitor content data, in relation to inquiries of serious crimes, as defined by national law. **Period covered: 01/10/2005 -** Articles concerned : 14 **Declaration contained in the instrument of ratification deposited on 21 June 2005 - Or. Engl.** Pursuant to Article 38 of the Convention, Denmark declares that, until further notice, the Convention will not apply to the Feroe Islands and Greenland. **Period covered: 01/10/2005 -** Articles concerned : 38 **Declaration contained in a letter from the Permanent Representative of Denmark, dated 28 September 2005, registered at the Secretariat General on 30 September 2005 – Or. Engl. and up-dated in a letter from the Minister of Foreign Affairs of Denmark, dated 1 August 2018, registered at the Secretariat General on 23 August 2018 – Or. Engl.** In accordance with Article 24, paragraph 7, of the Convention, the Government of the Kingdom of Denmark has designated as competent authority: the Rigsadvokaten (Director of Public Prosecution),

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Frederiksholms Kanal 16, DK-1220 Copenhagen K, Denmark, Tel: + 45 72 68 90 00 Fax: + 45 72 68 90 04 E-mail: rigsadvokaten@ankl.dk. **Period covered: 01/10/2005 -** Articles concerned : 24 **Declaration contained in a letter from the Permanent Representative of Denmark, dated 28 September 2005, registered at the Secretariat General on 30 September 2005 – Or. Engl. and up-dated in a letter from the Minister of Foreign Affairs of Denmark, dated 1 August 2018, registered at the Secretariat General on 23 August 2018 – Or. Engl.** In accordance with Article 27, paragraph 2, of the Convention, the Government of the Kingdom of Denmark has designated as competent authority: the Rigsadvokaten (Director of Public Prosecution), Frederiksholms Kanal 16, DK-1220 Copenhagen K, Denmark, Tel: + 45 72 68 90 00 Fax: + 45 72 68 90 04 E-mail: rigsadvokaten@ankl.dk. **Period covered: 01/10/2005 -** Articles concerned : 27 **Declaration contained in a letter from the Permanent Representative of Denmark, dated 28 September 2005, registered at the Secretariat General on 30 September 2005 – Or. Engl.** In accordance with Article 35, paragraph 1, of the Convention, the Government of the Kingdom of Denmark has designated as competent authority: The Danish National Police Police Department Polititorvet 14,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	DK-1780 Copenhagen V Denmark **[Note by the Secretariat**: For more information please contact the Executive Secretary of the Cybercrime Convention Committee, alexander.seger@coe.int.**]** **Period covered: 01/10/2005 -** Articles concerned : 35

Back to the Table of Contents