Netherlands

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 01 May 2020

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	
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	***Section 138ab***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	1.Any person who intentionally and unlawfully gains entry to a computerised device or system or a part thereof shall be guilty of computer trespass and shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category. Unlawful entry shall be deemed to have been committed if access to the computerised device or system is gained: a.by breaching a security measure, b.by a technical intervention, c.by means of false signals or a false key, or d.by assuming a false identity. 2.Computer trespass shall be punishable by a term of imprisonment not exceeding four years or a ine of the fourth category, if the offender subsequently copies the data stored, processed or transferred by means of the computerised device or system , which he has unlawfully accessed, and copies, intercepts or records such data for his own use or that of another. 3.Computer trespass committed via a public telecommunication network shall be punishable by a term of imprisonment not exceeding four years or a fine of the fourth category, if the offender subsequently a.with the intentionof benefitting himself or anotherunlawfully,uses processing capacity of a computerised device or system; b.accesses the computerised device or system of a third party via the computerised device or system to which he has unlawfully gained entry.
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	**Section 139c** 1.Any person who intentionally and unlawfully intercepts or records by means of a technical device data which is not intended for him and is processed or transferred by means of telecommunication or by means

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	of a computerised device or system,shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category. 2.Subsection (1) shall not apply to intercepting or recording: 1°data received via a radio receiver, unless a special effort was made or a prohibited receiver was used to enable such reception; 2°.by or on the instructions of the person entitled to use the telecommunication connection, except in cases of obvious isuse; 3°.for the purpose of a good operation of a public telecommunication network, for the purpose of criminal proceedings, or for the purpose of implementation of the Intelligence and Security Services Act 2002.
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.	**Section 350a** 1.Any person who intentionally and unlawfully alters, erases, renders unusable or disables data stored, processed or transferred by means of a computerised device or system or by means of telecommunication, or adds other data thereto, shall be liable to a term of imprisonment not exceeding two years or a fine of the fourth category. 2.Any person who commits the offence defined in subsection (1) after having unlawfully gained access, through a public telecommunication network, to a computerised device or system, and causes serious damage to such data, shall be liable to a term of imprisonment not exceeding four years or a fine of the fourth category. 3.Any person who intentionally and unlawfully makes available or disseminates data that is intended to cause damage in a computerised device or system, shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category. 4.Any person who commits the offence defined in subsection (3) with the intention of limiting the damage resulting from such data shall not be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	criminally liable.
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	**Section 138b** Any person who intentionally and unlawfully hinders the access to or use of a computerised device or system by offering or sending data to it **Section 350a** 1. Any person who intentionally and unlawfully alters, erases, renders unusable or disables data stored, processed or transferred by means of a computerised device or system or by means of telecommunication, or adds other data thereto
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	**139d par** 2) Any person who: a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offence, or b. sells, obtains, distributes or otherwise makes available or has in his possession a computer password, access code or similar data that can be used for accessing a computerised device or system or a part thereof;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Art. 326/225 (phishing, fraud on online markets, advance fee fraud, "click" fraud), 232 (skimming), 310 (theft of virtual goods) 317/318/285 (embezzlement, / blackmail), 334 (market manipulation), 139e (fencing) Dutch Criminal Code** **(326)** Any person who, with the intention of benefitting himself or another person unlawfully, either by assuming a false name or a false capacity, or by cunning manoeuvres, or by a tissue of lies, induces a person to hand over any property, to render a service, to make available data, to incur a debt or relinquish a claim; **(232)** Any person who intentionally makes a false cash card, a stored value card, any other card available to the public or an identity data carrier available to the public that is intended for making or obtaining automated payments or other services, or falsifies such card or carrier, with the intention of benefiting himself or another, Any person who intentionally uses the false or falsified pass or card as if it were genuine and unfalsified or intentionally delivers, possesses, receives, obtains, transports, sells or transfers such pass or card, while he knows or has reasonable cause to suspect that the pass or card is destined for such use

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(310) Any person who takes any property belonging in whole or in part to another person with the intention of unlawfully appropriating
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.	**Art. 326/225 (phishing, fraud on online markets, advance fee fraud, "click" fraud), 232 (skimming), 310 (theft of virtual goods) 317/318/285 (embezzlement, / blackmail), 334 (market manipulation), 139e (fencing) Dutch Criminal Code** **(326)** Any person who, with the intention of benefitting himself or another person unlawfully, either by assuming a false name or a false capacity, or by cunning manoeuvres, or by a tissue of lies, induces a person to hand over any property, to render a service, to make available data, to incur a debt or relinquish a claim; **(232)** Any person who intentionally makes a false cash card, a stored value card, any other card available to the public or an identity data carrier available to the public that is intended for making or obtaining automated payments or other services, or falsifies such card or carrier, with the intention of benefiting himself or another, Any person who intentionally uses the false or falsified pass or card as if it were genuine and unfalsified or intentionally delivers, possesses, receives, obtains, transports, sells or transfers such pass or card, while he knows or has reasonable cause to suspect that the pass or card is destined for such use **(310)** Any person who takes any property belonging in whole or in part to another

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	person with the intention of unlawfully appropriating
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**Section 240b** 1.Any person who distributes, offers, publicly displays, produces, imports, conveys in transit, exports, obtains, possesses or accesses by means of a computerised device or system or by use of a communication service an image or a data carrier that contains an image of a sexual act involving or seemingly involving a person who is manifestly under the age of eighteen years, shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category. 2.Any person who makes a profession or habit of committing any of the serious offences defined in subsection (1), shall be liable to a term of imprisonment not exceeding eight years or a fine of the fifth category
Title 4 – Offences related to infringements of copyright and related rights	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	Dutch Copyright Act
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
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.	
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
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.	**Article 126ni of Dutch Code of Criminal Procedure** A specific provision is available with Article 126ni of Dutch Code of Criminal Procedure. The procedure is described in article 126 ni DCCP itself. The request is delivered by the prosecution office either orally or in writing. When delivered orally, a written version is to be transferred to the requested party within 3 days and is signed by a prosecutor. The written request stipulates: a.An accurate description of the data to be preserved; b.Date, time of request c.The grounds that justify the request d.The period of requested preservation e.Whether the request also involves data necessary for retrieving the identity of other providers whose networks or services were used in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	the relevant communication. The public prosecutor makes a report on his request. The measure is available for crimes for which pretrial detention is possible
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	The Netherlands have adopted a specific provision in Article 126ni (paragraph 2) of the CPC. The DCCP enables the public prosecutor, in cases of crimes for which pre-trial detention is allowed (these include almost all cybercrimes) and which seriously infringe the rule of law, to order someone to preserve data stored in a computer that are particularly vulnerable to loss or change. If the data relate to communications, the communications provider is also required to provide the data necessary for retrieving the identity of other providers whose networks or services were used in the relevant communication.
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.	**Section 126n** 1. In the case of suspicion of a serious offence as defined in section 67(1), the public prosecutor may, in the interest of the investigation, request the provision of data on a user of a communication service and the communication traffic data pertaining to that user. The request may only relate to data designated by Governmental Decree and may involve data which: a.was processed at the time of the request, or b.is processed after the time of the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	2.The request, referred to in subsection (1), may be directed to any provider of a communication service. Section 96a(3) shall apply mutatis mutandis. 3.If the request relates to data as referred to in subsection (1, second sentence)(b), the request shall be made for a period of maximum three months. 4.The public prosecutor shall have an official record of the request prepared, which shall state: a.the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b.the facts or circumstances which show that the conditions, referred to in subsection (1), have been met; c. if known, the name or otherwise the most precise description possible of the person about whom data is requested; d.the data requested; e.if the request relates to data as referred to in subsection (1, second sentence)(b), the period to which the request relates. 5.If the request relates to data referred to in subsection (1, second sentence)(b), the request shall be terminated as soon as the conditions, referred to in subsection (1, first sentence), are no longer met. The public prosecutor shall have an official record made of amendment, supplementation, extension or cancellation of the request. 6.Rules pertaining to the manner in which the public prosecutor requests data may be set by Governmental Decree. **Section 126na** 1.In the case of suspicion of a serious offence, the investigating officer may, in the interest of the investigation, request the provision of data pertaining to name, address, postal code, town, number and type of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	service of a user of a communication service. Section 126n(2) shall apply. 2.If the data, referred to in subsection (1), is not known to the provider and is necessary for the application of section 126m or section 126n, the public prosecutor may, in the interest of the investigation, request the provider to retrieve and provide the requested data in a manner to be determined by Governmental Decree. 3.In the case of a request, as referred to in subsection (1) or (2), section 126n(4)(a)(b)(c) and (d) shall apply mutatis mutandis and section 126bb shall not apply. 4.Rules pertaining to the manner in which the investigating officer or the public prosecutor will request the data may be set by or pursuant to Governmental Decree. **Section 126nb** 1.In order to be able to apply section 126m or section 126n, the public prosecutor may, subject to section 3.10(4) of the Telecommunications Act, order that the number by which the user of a communication service can be indentified will be obtained by means of equipment referred to in that section. 2.The warrant shall be issued to a civil servant as referred to in section 3.10(4)(a) of the Telecommunications Act and shall be in writing. In the case of urgent necessity the warrant may be issued verbally. In that case the public prosecutor shall put the warrant in writing within three days. 3.The warrant shall be issued for a period of maximum one week and shall state: a.the facts or circumstances which show that the conditions for the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	application of section 126m or section 126n have been met and b.the name or the most precise description possible of the user of a communication service whose number has to be obtained. 4.The public prosecutor shall have others destroy, in his presence, the official records or other objects, from which information can be derived that was obtained through application of subsection(1), if that information is not used for the purpose of application of section 12 6m or section 126n
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be	**125i DCCP** The power to search a place for the purpose of recoding data stored or recorded in a data carrier at this place shall be conferred on the examining magistrate, the public prosecutor, the assistant public prosecutor and the investigating officer under the same conditions as referred to in sections 96b, 96c(1), (2) and (3), 97 (1) to (4) inclusive, and 110 (1) and (2). They may record this data in the interest of the investigation. Sections 96(2), 98, 99 and 99a shall apply mutatis mutandis.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**126m DCCP** 1.In the case of suspicion of a serious offence as defined in section 67(1), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required by the investigation, order an investigating officer to record by means of a technical device non-public communications which are conducted by use of the services of a provider of a communication service. 2.The warrant shall be in writing and shall state: a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b.the facts or circumstances which show that the conditions, referred to in subsection (1), have been met; c.where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user; d.the term of validity of the warrant; e.a description of the nature of the technical device orthe technical devices by means of which the communications are recorded. 3.If the warrant relates to communications which are conducted through a public telecommunication network or by use of a public telecommunication service within the meaning of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Telecommunications Act, the warrant shall – unless such is impossible or is not permitted in the interest of the criminal proceedings –be executed with the assistance of the provider of the public elecommunication network or the public telecommunication service and the warrant shall be accompanied by the request for assistance from the public prosecutor to the provider. 4.If the warrant relates to communications other than the communications referred to in subsection (3), the provider shall –unless suchis impossible or is not permitted in the interest of the criminal proceedings –be given the opportunity to assist in the execution of the warrant. 5.The warrant, referred to in subsection (1), may only be issued following written authorisation to be granted by the examining magistrate on application of the public prosecutor. Section 126l(5) to (8) inclusive shall apply mutatis mutandis. 6.Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumedto have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption. 7.The request referred to in subsection (6) shall not be directed to the suspect. 8.Section 96a(3) and section 126l(4), (6) and (7) shall apply mutatis mutandis to the request referred to in subsection (6). 9.Rules pertaining to the manner in which the order referred to in subsection (1) and the requests referred to in subsections (3) and (6) may be given and the manner of compliance with such requests shall be set by Governmental Decree.
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	**126m DCCP** 1.In the case of suspicion of a serious offence as defined in section

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	67(1), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required by the investigation, order an investigating officer to record by means of a technical device non-public communications which are conducted by use of the services of a provider of a communication service. 2.The warrant shall be in writing and shall state: a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b.the facts or circumstances which show that the conditions, referred to in subsection (1), have been met; c.where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user; d.the term of validity of the warrant; e.a description of the nature of the technical device orthe technical devices by means of which the communications are recorded. 3.If the warrant relates to communications which are conducted through a public telecommunication network or by use of a public telecommunication service within the meaning of the Telecommunications Act, the warrant shall – unless such is impossible or is not permitted in the interest of the criminal proceedings –be executed with the assistance of the provider of the public elecommunication network or the public telecommunication service and the warrant shall be accompanied by the request for assistance from the public prosecutor to the provider. 4.If the warrant relates to communications other than the communications referred to in subsection (3), the provider shall –unless suchis impossible or is not permitted in the interest of the criminal

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	proceedings –be given the opportunity to assist in the execution of the warrant. 5.The warrant, referred to in subsection (1), may only be issued following written authorisation to be granted by the examining magistrate on application of the public prosecutor. Section 126l(5) to (8) inclusive shall apply mutatis mutandis. 6.Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumedto have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption. 7.The request referred to in subsection (6) shall not be directed to the suspect. 8.Section 96a(3) and section 126l(4), (6) and (7) shall apply mutatis mutandis to the request referred to in subsection (6). 9.Rules pertaining to the manner in which the order referred to in subsection (1) and the requests referred to in subsections (3) and (6) may be given and the manner of compliance with such requests shall be set by Governmental Decree.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.	**DCC** Section 2 The criminal law of the Netherlands shall apply to any person who commits a criminal offence in the Netherlands. Section 3 The criminal law of the Netherlands shall apply to any person who commits a criminal offence on board a Dutch vessel or aircraft outside

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 territory of the Netherlands. Section 4 The criminal law of the Netherlands shall apply to any person who commits outside the territory of the Netherlands: Par 1-17
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis	**Section 552hh** 1. A request for extradition of a person who is in the Netherlands and who is suspected or has been convicted of a criminal offence, referred to in any of the provisions of the treaties referred to in subsection (2), shall be regarded as a request for the institution of criminal proceedings which has been granted, if that request is from a state which is bound to the provisions of the treaty concerned and if the extradition is declared inadmissible by court judgment or the request is refused by Ministerial Order. 2.Subsection (1) shall pertain to criminal offences, referred to in: - article 1 of the European Convention on the Suppression of Terrorism (Treaty Series1977, 63); - articles 5, 6, 7 and 9 of the European Convention on the Prevention of terrorism (Treaty Series 2006, 34).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	3.The provisions of section 552y(1, opening lines) and (a) shall not apply to a request as referred to in the final passage of subsection (1). 4.In addition, the provisions of section 552y(1, opening lines) and (b)(2e) shall not apply to requests based on the European Convention on the Prevention of Terrorism and on the Agreement concerning Application of that Convention among the Member States of the European Communities (Treaty Series 1980, 14).
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	Section 552h-552q CCP

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 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	**Article 552i CCP** 1.If the request is not addressed to a public prosecutor, the addressee shall promptly forward it to the public prosecutor in the district where the requested act must be conducted, or where the request was received, or to a public prosecutor at theNational Office of the Public Prosecution Service or the National Office of the Public Prosecution Service for Financial, Economic and Environmental Offences. 2.The request shall not be required to be forwarded if it pertains solely to information and the coercive measures or powers, as referred to in sections 126g to 126z inclusive, sections 126zd to 126zu inclusive and section 126gg, or the application of section 126ff, are not necessary in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	order to obtain such information. 3. An entry shall be made of each request granted, in accordance with subsection (2), in a register in a format to be established by Our Minister. The entry shall include, in any case, the nature of the request, the capacity of the person making the request and the action taken on therequest. 4.In the handling of a request the authority competent pursuant to subsection (2) shall observe the general and special instructions given by the public prosecutor.
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 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:	If no treaty exists, the Code of Criminal Procedure applies, and assistance is limited to measures that do not require coercion For non-treaty requetst, Article 552l CCP sets forth several bases for denial which include: Reason to suspect an investigation/prosecution is to punish for regilious, ideological or political belief or nationality or race Conviction for the same crime The requests is for investigation of an offense for which the individual is being prosecuted in the Netherlands

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b 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). 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	If no treaty exists, the Code of Criminal Procedure applies, and assistance is limited to measures that do not require coercion. DCCP has absolute and relative ground for refusal (article 552k, 552l, 552m DCCP)
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or	Article 126ni of DCCP for domestic preservation may also be used for international requests. The public prosecutor is competent for receiving and executing request. The prosecutor needs to be convinced that there are grounds for a request for preservation. is the focal point (24/7) for cybercrime and will contact partners in order to have a preservation order.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**DCC Section 126n** 1. In the case of suspicion of a serious offence as defined in section 67(1), the public prosecutor may, in the interest of the investigation, request the provision of data on a user of a communication service and the communication traffic data pertaining to that user. The request may only relate to data designated by Governmental Decree and may involve data which: a.was processed at the time of the request, or b.is processed after the time of the request. 2.The request, referred to in subsection (1), may be directed to any provider of a communication service. Section 96a(3) shall apply mutatis mutandis. 3.If the request relates to data as referred to in subsection (1, second sentence)(b), the request shall be made for a period of maximum three months. 4.The public prosecutor shall have an official record of the request prepared, which shall state: a.the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b.the facts or circumstances which show that the conditions, referred to in subsection (1), have been met; c.if known, the name or otherwise the most precise description possible of the person about whom data is requested; d.the data requested; e.if the request relates to data as referred to in subsection (1, second sentence)(b), the period to which the request relates. 5.If the request relates to data referred to in subsection (1, second sentence)(b), the request shall be terminated as soon as the conditions, referred to in subsection (1, first sentence), are no longer met. The public prosecutor shall have an official record made of amendment, supplementation, extension or cancellation of the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	6.Rules pertaining to the manner in which the public prosecutor requests data may be set by Governmental Decree.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**General provisions regarding MLA: Section 552h-552q CCP** Preservation of computer data (art. 126ni DCCP) Art. 126ni DCCP enables the public prosecutor, in cases of crimes for which pre-trial detention is allowed and which seriously infringe the rule of law, to order someone to preserve data stored in a computer that are particularly vulnerable to loss or change. The preservation can be ordered for a period of at most 90 days (extendible once). Search and seizure of information system/computer data (general seizure provisions art. 95, 96, 96a, and 104 DCCP, art. 125i power to search in order to preserve data, 125j DCCP power to conduct a network serach)
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.	**General provisions regarding MLA: Section 552h-552q CCP** real-time interception/collection of traffic/content data; Art. 126m DCCP enables the public prosecutor, with authorization from a judge, to order the recording of communications that are generated by means of a communications service provider's service. Interception is permitted in cases for which pre-trial detention is allowed and which seriously infringe the rule of law. If the intercepted communications turn out to be encrypted, an order to decrypt may be directed at the person

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	who is likely to know the decryption means, but not at the suspect, according to art. 126m para. 6 and 7 DCCP.
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.	**General provisions regarding MLA: Section 552h-552q CCP** real-time interception/collection of traffic/content data; Art. 126m DCCP enables the public prosecutor, with authorization from a judge, to order the recording of communications that are generated by means of a communications service provider's service. Interception is permitted in cases for which pre-trial detention is allowed and which seriously infringe the rule of law. If the intercepted communications turn out to be encrypted, an order to decrypt may be directed at the person who is likely to know the decryption means, but not at the suspect, according to art. 126m para. 6 and 7 DCCP.
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	Implemented. National High Tech Crime Unit ,National Police Postal address: p.o.box 11, 3970 AA, Driebergen, The Netherlands

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	

Back to the Table of Contents