# Criminal Justice (Protection, Preservation of and Access to Data on Information Systems) Bill 2024

## General Scheme

## Arrangements of Heads

## Contents

# Part 1 – General

## Head 1 - Short Title, Commencement and Transitional Provisions

(1) This Act may be cited as the Criminal Justice (Protection, Preservation of and Access to Data on Information Systems) Act 2024.

(2) This Act shall come into operation on such day or days as the Minister for Justice may appoint by order or orders either generally or with reference to any particular purpose or provision and different days may be so appointed for different purposes or different provisions.

(3) The amendments made by Head 7B of this Scheme shall not apply to requests sent by the Minister to the Commissioner of An Garda Síochána pursuant to section 75 (5) of the Act 2008 before the commencement of Head 7B,

***Explanatory Note***

*This is a standard provision.*

## Head 2 – Interpretation

"Act of 2008" means the Criminal Justice (Mutual Assistance) Act 2008 as amended;

"Act of 2011" means the Communications (Retention of Data) Act 2011 as amended;

"Act of 2017" means the Criminal Justice (Offences Relating to Information Systems) Act 2017;

"authorised person" means

- A member of an Garda Síochána ;
- In the case of a competition offence, an officer of the Competition and Consumer Protection Commission not below the rank of assistant principal officer;
- In the case of a revenue offence, an officer of the Revenue Commissioners not below the rank of assistant principal officer:
- [In the case of a criminal investigation by Fiosrú - Oifig an Ombudsman Póilíneachta, a member of Fiosrú - Oifig an Ombudsman Póilíneachta;]
- An officer authorised by the Corporate Enforcement Authority

"Budapest Convention" means the Convention on Cybercrime signed at Budapest on 23rd day of November 2001;

"competition offence" has the same meaning as in the Act of 2011;

"content data" means any data in a digital format including text, voice videos, images and sound other than subscriber or traffic data;

"data" has the same meaning as in the Act of 2017;

"data requested for the sole purpose of identifying the user" means Internet Protocol addresses and, where necessary, the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers and related information where requested by law enforcement authorities for the sole purpose of identifying the users in a specific criminal investigation;

"designated judge" means a judge designated under Head 2A;

"electronic communications service" has the same meaning as in the Act of 2011;

"electronic evidence" means subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form;

"information system" has the same meaning as in the Act of 2017;

"revenue offence" has the same meaning as in the Act of 2011;

"serious offence" has the same meaning as in the Act of 2011;

"service provider" means a person that provides one or more of the following categories of services:

(a) electronic communications service
(b) internet domain name and, Internet Protocol numbering services such as, Internet Protocol address providers, domain name registries, domain name registrars and domain name related privacy and proxy services;
(c) other services that provide the ability to its users to communicate with each other or the ability to process or store data on behalf of the users to whom the service is provided for, where the storage of data is a defining component of the service provided to the user;

"subscriber data" means any data held by a service provider relating to the subscription to the services, pertaining to:

(a) the identity of a subscriber or customer including where appropriate the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, email address, Internet Protocol address, the International Mobile Subscriber Identifier or the International Mobile Equipment Identity
(b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer at the moment of initial registration or activation, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user.

"traffic data" means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression including electronic communications metadata and data relating to the commencement and termination of a user access session to a service such as the date and time of use, the log-in to and log-off from the service other than subscriber data.

## *Explanatory Note*

*This Head deals with definitions that are used throughout the general scheme. The terminology used is intended to meet requirements of the Convention on Cybercrime signed at Budapest on 23rd day of November 2001(the Budapest Convention) and Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (the E-evidence Regulation), which involve measures that this scheme gives effect to.*

*The Criminal Justice (Offences Relating to Information Systems) Act 2017 (the 2017 Act) deals with cybercrime offences and already gives effect to aspects of the Budapest Convention hence why some of its definitions are shared with this Bill.*

*There is crossover also over with the definitions in the Communications (Retention of Data) Act 2011, as amended by the Communications (Retention of Data) (Amendment) Act 2022 (the 2011 Act as amended), as that Act also provides for production and preservation orders in relation to electronic data/evidence. However the definitions used in the Bill in relation to the data categories, while overlapping in terms of meaning with those in the 2011 Act (as amended), replicate the terminology in the E.U. E-evidence Regulation and the Budapest Convention, so as to ensure there is no ambiguity with regards compliance. Of particular importance is the definition of "content data", a new data category not previously covered by the 2011 Act (as amended) production and preservation order regime and that the orders in this Bill will cover.*

## Head 2A – Designated Judge

(1) The President of the District Court may designate such and so many judges of the District Court to be a designated judge for the purposes of

(a) Part 2 [or]
(b) Part 3

of this Scheme.

(2) An application to a designated judge under Head 5, Head 6 or Head 12 may be made

(a) Whether or not the service provider in respect of whom the application is made is resident or located in the District Court district to which the designated judge stands assigned, and
(b) Whether or not the data in respect of which the application is made is retained by the service provider within the District Court district to which the designated judge stands assigned.

### *Explanatory Note*

*This Head deals with the designation of District Court judges for the specific purposes of issuing:*

- *domestic production/preservation orders – orders applied for by Irish authorities in respect of data controlled by service providers based in Ireland (1 (a)), and;*
- *European Production/Preservation orders – orders applied for by Irish authorities in respect data controlled by service providers based in another EU country (1(b))*

*Specifically designated District Court judges are intended to be an option for the issuing of domestic production/preservation orders. An alternative will be the issuing of these orders by District Court judges selected based on geographical jurisdiction e.g. a judge in whose District the service provider with control of the data is based (see Head 6B).*

*In respect of European Production/Preservation orders, it is intended that only specifically designated judges will issue the orders, as the addressee of the order will be outside the traditional geographical jurisdiction of all Irish courts, so there is no natural geographical jurisdictional base for the District Court.*

## Head 3 – Expenses

The expenses incurred by the Minister in the administration of this Act [other than Part 4] shall, to such extent as may be sanctioned by the Minister for Public Expenditure, National Development Plan Delivery and Reform, be paid out of moneys provided by the Oireachtas.

***Explanatory Note:***

*This is a standard provision.*

## Part 2 – Budapest Convention

### Head 4 – Possession of item for commission of certain offences

(1) A person, who without lawful authority or reasonable excuse, is in possession of any computer programme, device, key, code or data referred to by paragraph (a) or (b) of section 6 of the Act of 2017 shall be guilty of an offence.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that at the time of the alleged offence the computer programme, device, key, code or data referred to by paragraph (a) or (b) of section 6 of the Act of 2017 was not in his or her possession for the purpose of the commission of an offence under section 2, 3, 4, or 5 of the Act of 2017.

(3) A person who commits an offence under this section shall be liable to

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years or both.

***Explanatory Note***

*This Head provides for the offence of possession of an item for the purpose of committing any of the offences covered by articles 2-5 of the Budapest Convention (cybercrime offences). The cybercrime offences were already covered by Irish law (sections 2-5 of the 2017 Act), but the possession offence was not and is a requirement of Article 6 of the Budapest Convention.*

## Head 5 – Preservation of data

(1) This Head applies to data stored on or accessible by an information system, other than data retained solely in accordance with section 3A or section 7A(3) or section 7B(3) of the Act of 2011.

(2) An authorised person may apply to a judge of the District Court, who has jurisdiction in accordance with Head 6B, for a preservation order in respect of subscriber data or data requested for the sole purpose of identifying the user where the applicant is of the belief that data in respect of which the application is made

(a) relates to a person whom the applicant suspects upon reasonable grounds of having committed a criminal offence, in the State or elsewhere that would attracts a penalty of six months imprisonment or more in the State, or
(b) is required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a criminal offence in the State or elsewhere that would attract a penalty of six months imprisonment or more in the State or apprehending a person who has committed such an offence, and the data is vulnerable to loss or modification.

(3) An authorised person may apply to a judge of the District Court, who has jurisdiction in accordance with Head 6B, for a preservation order in respect of traffic data or content data where the applicant is of the belief that data in respect of which the application is made

(a) relates to a person whom the applicant suspects upon reasonable grounds of having committed a serious offence in the State or elsewhere, or
(b) is required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a serious offence or apprehending a person who has committed such an offence, in the State or elsewhere, and the data is vulnerable to loss or modification.

(4)

(a) Subject to Head 6C, an application for a Preservation Order pursuant to subheads (2) or (3) shall -

(i) be made ex parte,
(ii) be upon information on oath specifying:

A. the addressee or addressees of the Preservation Order;
B. the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, login ID or account name;
C. details of data to be preserved including whether the data sought to be preserved is subscriber data, data requested for the sole purpose of identifying the user, traffic data or content data;
D. if applicable, the time range requested to be preserved;

E. the criminal offence to which it relates or if it relates to the execution of a custodial sentence or detention order, details of the offence, conviction and sentence imposed;
F. the grounds for the necessity and proportionality of the measure, including why the data being sought to be preserved is regarded as vulnerable to removal, deletion or alteration;
G. whether or not there is any reasonable indication that any of the data sought may be subject to privilege from disclosure in criminal proceedings,

(iii) be heard otherwise than in public.

(b) Where the application does indicate that any of the data sought may be subject to privilege from disclosure in criminal proceedings, the provisions of Head 6A shall apply, including Head 6A(6).

(5)

(a) An application for a Preservation Order may be made pursuant to subheads (2) or (3) by an authorised person on behalf of the competent authority of another state where a request meeting the requirements set out in paragraph (b) has been received to obtain the expeditious preservation of data stored in the State or under the control of a person in the State.
(b) A request from another state shall specify the authority seeking the preservation, the offence that is the subject of criminal investigation or proceedings, the data to be preserved, the person or persons in control of the data or the location where the data is stored, the necessity for preservation and shall include a statement that it is intended that a mutual assistance request will be submitted by that other state for the search for, seizure or production of the data.
(c) For the purpose of an application pursuant to subsections (2) or (3) on behalf of the competent authority of another state, the authorised person making the application may form his or her belief that the data in respect of which the application is made relates to a person whom the applicant suspects upon reasonable grounds of having committed a relevant offence, or is required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a relevant offence or apprehending a person who has committed such an offence and the data is vulnerable to loss or modification on the basis of the material supplied by the authorities in the other state in support of the request.
(d) Delays associated with the processing of a mutual assistance request may be a factor to be taken into account when determining that data is vulnerable to loss or modification.

(6) The judge, as respects an application under subheads (2) or (3), may make a preservation order under this subhead only if satisfied that

(a) The requirements of subheads (2) or (3), as the case may be, applies to the data in respect of which the application is made,
(b) the data is vulnerable to loss or modification, and
(c) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(7)

(a) A preservation order under this section, shall, while it is in effect, require the service provider or person specified in the order to preserve the category and class of data in his or her possession or control at the time of receipt of the order in accordance with such conditions and directions as may be specified in the order.

(b)

(i) A preservation order under this section relating to traffic data, shall require the service provider or person specified in the order to determine if, to his or her knowledge, a service provider other than that specified in the order was involved in the transmission of the communication or communications which are the subject of the order and if so shall expeditiously disclose to the authorising person who made the application a sufficient amount of traffic data to identify the other service providers involved and the path through which the communication was transmitted.

(ii) In a case to which subparagraph (i) applies where the application was made on behalf of the competent authority of another state, the authorised person shall advise the competent authority of the requesting state of this fact and shall supply a sufficient amount of traffic data available to that authority that identifies the service provider in the other state and the path through which the communication was transmitted outside the State.

(8) For the purposes of subhead (7)(a), a judge may specify the category and class of data by reference to one or more of the following:

(a) subscriber data, data requested for the sole purpose of identifying the user, traffic data, content data;
(b) a particular location or locations;
(c) a particular period of time;
(d) a particular means of communication;
(e) a particular person or persons, user name or usernames;
(f) a particular Internet Protocol address or addresses;
(g) such other matter or feature as the judge considers appropriate.

(9)

(a) Subject to paragraph (b) and (c) a preservation order shall have effect for 90 days, or such lesser period as may be specified in the order.

(b) If a preservation order was made at the request of the competent authority of another state and a mutual assistance request has been submitted by that state to the Department of Justice in respect of the data in question, within 60 days of the making of the preservation order, the preservation order shall continue to have effect pending the outcome of that mutual assistance request.

(c) A preservation order made by a judge pursuant to this Head, where a question of privilege needs to be determined, or pursuant to Head 6(5) shall continue to have effect until discharged by the judge.

(10) Where a preservation order is made under this Head, the applicant concerned shall, without delay, cause the order to be served on the service provider or other person or persons specified in the order.

(11) A service provider or other person on whom a preservation order under this section is served shall as soon as possible comply with the order.

## *Explanatory Note*

*This Head provides for a general power to order the preservation of specific data for a short period (90 days) with a view to it being subject to a production order. Both the Budapest Convention and EU E-evidence Regulation require this.*

*The only existing preservation order of this type is section 7A and section 7B of the 2011 Act (as amended). While some of the procedural aspects of this Head mimic those corresponding sections in the 2011 Act (as amended), the provisions in the 2011 Act (as amended) do not cover content data, do not address the issues of communication pathways involving multiple service providers and do not provide for mutual assistance. This Head provides for these matters, as is required by the Budapest Convention.*

***Subhead (1)** is intended to exclude data retained solely on security grounds pursuant to Act of 2011 (as amended) so that there is no conflict with our data retention regime.*

***Subheads (2) and (3)*** *regulate who can apply for a preservation order, to whom the application should be made and in what circumstances. The lower severity crime threshold for subscriber data/data requested for the sole purpose of identifying the user versus traffic/content data reflect the greater degree of invasiveness of the latter data categories.*

***Subhead (4)*** *sets out the procedure to be followed for an application.*

***Subhead (5)*** *is intended to give effect to article 29 of the Budapest Convention providing a mechanism for the expedited preservation of stored computer data on behalf of the competent authority of another state. A formal request with details is required but it is envisaged that this can be made through police to police channels (informal mutual assistance) without the need for a formal mutual assistance request. It is a provisional measure, which does not provide for the release of sensitive data and is dependent on an undertaking that the data preserved will be sought by a formal mutual assistance request.*

***Subhead (6)*** *ensures that a preservation order may be made if the requirements of subhead (2) and (3) are met and it is necessary and proportionate.*

***Subhead (7)(a)*** *provides for the preservation of the data on foot of an order**.***

***Subhead (7)(b)*** *imposes a specific obligation on the service provider not only to preserve the data but also to check the pathway of the communication in question and advise the applicant if other service providers, not known to the applicant, are involved be they in the State or elsewhere.*

***Subhead (8)*** *outlines the types of requirements that a judge may include in an order and mimics the detail that should be in an application.*

***Subhead (9)(a)*** *sets out a 90 day limit on the preservation order.*

***Subhead (9)(b)*** *enables a preservation order to remain in force beyond the normal limit if a mutual assistance request has been received to allow the request to be processed.*

***Subhead (9)(c)*** *relates to data where the question of whether the data is privileged from disclosure in criminal proceedings (legal, journalistic) may apply and the data needs to be preserved for an extended period while the issue of privilege is determined (see Head 6A).*

***Subhead (10)*** *is straight forward requiring the applicant of the order to serve it on the addressee.*

***Subhead (11)*** *places a legal obligation on the recipient of the order to comply. An offence provision covering non-compliance of this subhead and Head 6 (production order) is included at Head 9 (Offences).*

## Head 6 – Production Orders

(1)

(a) This Head applies to data stored on or accessible by an information system, other than data retained solely in accordance with section 3A or section 7A(3) or section 7B(3) of the Act of 2011.

(b) This Head is without prejudice to any other statutory provision that allows for search warrant or production orders to be issued in respect of data stored on or accessible by an information system.

(2) An authorised person may apply to a judge of the District Court, who has jurisdiction in accordance with Head 6B, for a production order in respect of subscriber data or data requested for the sole purpose of identifying the user where the applicant is of the belief that data in respect of which the application is made

(a) relates to a person whom the applicant suspects upon reasonable grounds of having committed a criminal offence that attracts a penalty of six months imprisonment or more, or

(b) is required for the purpose of preventing, detecting, investigating or prosecuting a criminal offence, that attracts a penalty of six months imprisonment or more or apprehending a person who has committed such an offence.

(3) An authorised person may apply to a judge of the District Court, who has jurisdiction in accordance with Head 6B, for a production order in respect of traffic data or content data where the applicant is of the belief that data in respect of which the application is made

(a) relates to a person whom the applicant suspects upon reasonable grounds of having committed a serious offence, or

(b) is required for the purpose of preventing, detecting, investigating or prosecuting a serious offence or apprehending a person who has committed such an offence.

(4) Subject to Head 6A an application for a Production Order pursuant to subheads (2) or (3) shall -

(a) be made ex parte,

(b) be upon information on oath specifying:

(i) the addressee of the Production Order;

(ii) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, login identity or account name;

(iii) details of data sought including whether the data sought is subscriber data, data requested for the sole purpose of identifying the user, traffic data or content data;

(iv) if applicable, the time range requested to be preserved;

(v) the criminal offence to which it relates or if it relates to the execution of a custodial sentence or detention order, details of the offence, conviction and sentence imposed;

(vi) the grounds for the necessity and proportionality of the measure;

(vii) a summary description of the case;

(viii) whether or not there is any reasonable indication that any of the data sought may be subject to privilege from disclosure in criminal proceedings,

(c) be heard otherwise than in public.

(5)

(a) The judge, as respects an application under subheads (2) or (3), may make a production order under this subhead only if satisfied that:

(i) paragraph (a) or (b) of subhead (2) or (3), as the case may be, applies to the data in respect of which the application is made, and

(ii) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(b) If the judge is of the view that question of privilege needs to be determined in respect of certain data sought, he or she may make a preservation order in respect of that data and the provisions of Head 5(7)(a), (8), (9)(c), (10) and (11) [Head 9, Head 10 and Head 11] shall apply as appropriate.

(6) A production order under this section, shall, while it is in effect, require the service provider or person specified in the order to preserve as soon as possible the relevant data in his or her possession or control at the time of receipt of the order in accordance such conditions and directions as may be specified in the order and to produce, as soon as practicable, to the person specified in the order the data in accordance such conditions and directions as may be specified in the order.

(7) For the purposes of subhead (6), a judge may specify the data to be produced by reference to one or more of the following:

(a) subscriber data, data requested for the sole purpose of identifying the user, traffic data, content data;
(b) a particular location or locations;
(c) a particular period of time;
(d) a particular means of communication;
(e) a particular person or persons, user name or usernames;
(f) a particular Internet Protocol address or addresses;
(g) the format in which the material is to be produced so that it is legible, comprehensible and accessible;
(h) such other matter or feature as the judge considers appropriate.

(8)

(a) A judge of the District Court, who has jurisdiction in accordance with Head 6B, may at a sitting of the Court vary or discharge an order under this Head on the application of an authorised person or any person to whom the order relates.

(b) A submission by the addressee of an order, that compliance with the order would conflict with an obligation under the applicable law of a third country, shall be a matter to be taken into consideration by the Court.

(9)

(a) Where a production order [or a preservation order] is made under this Head, the applicant concerned shall, without delay, cause the order to be served on the service provider or other person or persons specified in the order.

(b) A service provider or other person on whom a production order under this section is served shall comply with the order as soon as practicable and shall provide a

statement/certificate as appropriate as to the provenance of the data and where appropriate a statement that the criteria specified in subhead (11)(b) (i) to (iii) do not apply to the data furnished.

(10)

(a) Subject to Head 6A, subhead (5)(b) and paragraph (b) of this subhead, an order made under this section shall not confer any right to production of or access to any material subject to privilege from disclosure in criminal proceedings.

(b) Data may be ordered to be produced notwithstanding that it is apprehended that the data is privileged from disclosure in criminal proceedings, provided it is produced in such a manner whereby the confidentiality of the data can be maintained pending the determination by a court of the issue as to whether the data is privileged material.

(11)

(a) Subject to paragraph (b) and (c), any data obtained pursuant to an order made under this Head [or section 7C(8) of the 2011 Act or disclosed pursuant to section 6, section 6C, section 6D, section 6E(1)(a) of the Act of 2011] may, subject to Part V of the Data Protection Act 2018 be retained and used as evidence in proceedings.

(b) Data which was produced to an authorised person by a service provider, or to which such a member was given access, in accordance with an order under this section shall be admissible in any criminal proceedings as evidence of any fact therein of which direct oral evidence would be admissible unless the information—

(i) is privileged from disclosure in such proceedings,

(ii) was supplied to an authorised person by a person who would not be compellable to give evidence at the instance of the prosecution,

(iii) was compiled for the purposes or in contemplation of any—

I. criminal investigation,

II. investigation or inquiry carried out pursuant to or under any enactmen

III. civil or criminal proceedings, or

IV. proceedings of a disciplinary nature,

(iv) the requirements of the provisions mentioned in paragraph (c) are not complied with.

(c) References in sections 7 (notice of documentary evidence to be served on accused), 8 (admission and weight of documentary evidence) and 9 (admissibility of evidence as to credibility of supplier of information) of the Criminal Evidence Act 1992, to a document or information contained in it shall be construed as including references to material mentioned in paragraph (b) and the information contained in it, and those provisions shall have effect accordingly with any necessary modifications.

(12)

(a) statement made under subhead (9) shall be:

(i) signed by a person aged 18 or over

(ii) include a declaration that the statement is true to the best of his or her knowledge and that he or she made the statement knowing that he or she would be liable to criminal prosecution if he or she stated in it anything which he or she knew to be false or did not believe to be true

(iii) describe their position and how he or she is qualified to make the statement regarding the provenance of the data produced and

(iv) outline the matters relevant to the provenance of the data, including the operation of the system on which the data was stored, the period when it was generated and that the system was functioning during the relevant period.

(b) For the purpose of this subhead, "signed" shall include an electronic signature within the meaning of the Electronic Commerce Act 2000 [notwithstanding the provisions of section 10 or 11 of that Act].

(13) A statement purporting to be made under subhead (9) shall in any proceedings be sufficient evidence of the facts stated in it without any proof of any signature, until the contrary is proved.

(14) Where a statement made pursuant to subhead (9) is tendered in evidence and the person by whom the statement was made has stated in it anything which he or she knew to be false or did not believe to be true, that person shall be guilty of an offence and shall be liable on summary convictions of a Class A fine or to imprisonment for a term not exceeding twelve months or to both or on conviction on indictment to a fine or to imprisonment for a term not exceeding 5 years or to both.

## *Explanatory Note*

*This Head is intended to give effect to Article 18 of the Budapest Convention and the requirements of the E-evidence Regulation in relation to domestic orders to produce specific data.*

***Subhead (1)(a)** is intended to exclude data retained solely on security grounds pursuant to Act of 2011 (as amended) so that there is no conflict with our data retention regime.*

***Subhead (1)(b)** is intended to make it clear that the provision is in addition to any existing powers to obtain search warrants or production orders and does not limit their application in any way.*

***Subheads (2) and (3)** regulate who can apply for a production order, to whom the application should be made and in what circumstances. It follows the thresholds set out in Head 5.*

***Subhead (4)** sets out the procedure to be followed.*

***Subhead (5)(a)*** *requires the judge to ensure the requirements of subhead (2) and (3) are followed and that the issuing of the order is necessary and proportionate.*

***Subhead (5)(b)*** *is intended to provide for circumstances where a question of privilege has arisen and one option may be to order that the data be preserved (rather than produced) pending consideration of the issue by the High Court under Head 6A.*

***Subhead (6)*** *is intended to ensure that there is an onus on the addressee to preserve the data as soon as possible (i.e. while the order is being considered and processed) while allowing more time for production (as soon as practicable).*

***Subhead (7)*** *is similar to Head 5(8) in outlining the types of requirements that a judge may include in an order and mimics the detail that should be in an application. It also provides that the judge may specify the format of the material so that is accessible and in a format that can be used by the applicant.*

***Subhead (8)(a)*** *allows for a production order to be varied or discharged. It will be a matter for the court to decide what is necessary and proportionate (Head 6 (5)) having heard the evidence from both sides. It is also intended to provide a mechanism whereby a service provider may raise the question of a conflict of laws (Article 18 of the Budapest Convention requires parties to the convention to exert extra territorial jurisdiction over data outside its territory when a person in its territory has "possession or control" over the data).* ***Subhead (8)(b)*** *makes explicit reference to the question of the conflict of laws being a ground for consideration.*

***Subhead (9)*** *places a legal obligation on the addressee of the order to comply. An offence provision covering this subhead and Head 5(11) is addressed by Head 9. It also includes a provision about a statement to accompany the data certifying its provenance and that the prohibitions relating to admissibility specified in subhead (11)(b) (i) to (iii) do not apply to the data furnished.*

***Subhead (10)(a)*** *addresses the issue where material is known to be or claimed to be privileged.*

***Subhead 10(b)*** *is intended to ensure that subhead (a) does not rule out the production of data in such cases pending a determination by the court.*

***Subhead (11)(a)*** *confirms that the material obtained may be used as evidence in proceedings.*

***Subhead (11)(b)*** *provides that data shall be admissible in any criminal proceedings subject to certain conditions such as where material is provided by a service provider and it subsequently transpires some of the material is privileged (**Subhead (11)(b)(i)),** other standard considerations when determining the admissibility of documentary evidence **(Subhead (11) (b) (ii) and (iii))** and a requirement to follow subhead 11(c) **(Subhead 11(b)(iv).***

***Subhead (11)(c****) relates to safeguards around the admissibility of evidence*

***Subheads (12)–(14)*** *provide for proof of provenance by certificate and ties in with the provisions of subhead (11)(b).*

***Subhead (12)*** *outlines the minimum that should be included in the certificate. In particular it requires a declaration stating that the person making the statement is liable to criminal prosecution (Subhead (14) provides for the offence). Because of the variety of the content in the material and the variety of sources and developments in technology, it is not considered desirable or feasible to be too prescriptive as to what should be contained. It will be a matter for the courts to determine if statements are adequate to justify the admission of the material.*

***Subhead (13)*** *sets out the presumption that a statement shall be sufficient evidence of the facts stated in it until the contrary is proved.*

***Subhead (14)*** *makes it an offence to provide false evidence in a statement.*

## Head 6A - Privileged Data

(1)

(a) An authorised person who has made an application pursuant to Head 5 or 6 may make an application to the High Court for a determination whether specified data
- sought in the application;
- which is or has been made the subject of preservation order; or
- which is the subject of a production order;

is privileged from disclosure in criminal proceedings.

(b) In a case where the application for a preservation order or production order has been refused, or in the case preservation order has been made in respect of the data in question, an application under paragraph (a) shall be made within [14] days.

(2)

(a) A service provider who has been the addressee of a preservation or production order pursuant to Head 5 or 6 may make an application to the High Court for a determination whether data specified in such orders is privileged from disclosure in criminal proceedings.

(b) Such an application shall be made within [14] days after a preservation order or a production order has been served on the service provider.

(3) Where a preservation order or a production order has been made pursuant to Heads 5 and 6, the person
- who is the addressee of the order and is not a service provider,
- to whom the data, which is the subject of the order, relates,
- who provided the data to the service provider or
- who controls the data

may make an application to the High Court for a determination whether specified data in such orders is privileged from disclosure in criminal proceedings.

(4) Pending the making of a final determination on an application under subhead (1), (2) or (3), the High Court may give such interim or interlocutory directions as the court considers appropriate including, without prejudice to the generality of the foregoing directions, directions as to-

(a) The preservation of the data in whole or in part in a safe and secure place or storage device.

(b) The appointment of a person with suitable legal qualifications or technical skills possessing the level of experience and the independence from any interests falling to be determined for the purpose of
(i) examining the data, and
(ii) preparing a report for the court with a view to assisting or facilitating the court of its determination as to whether the data is privileged for the purpose of criminal proceedings.

(5) An application under subhead (1), (2) or (3) shall be by motion on notice and may if the court directs be heard otherwise than in public.

(6) In a case where a preservation order has been made pursuant to Head 5 or Head 6 (5) (b), and the High Court determines that the data in question is privileged for the purpose of criminal proceedings, the authorised person who made the application for the production order shall apply to the judge to discharge that order and notify the addressee of the preservation order of the decision of the judge.

## *Explanatory Note*

*This Head deals with the question of privilege in the context of an application for a domestic production order.*

***Subhead (1)** applies to an authorised person who has applied for an order, and a request by them for a determination regarding privilege in relation to the data. It is intended to cover 3 situations:*

- *An application for a production order has been made but refused by the judge because of a view that the data is privileged and the applicant wants to challenge that view in the High Court;*
- *An application for a production order has been made but only a preservation order has been granted and the applicant wants to have the matter of privilege determined in the High Court;*
- *An application for a production order has been made and granted and having received the data, the applicant realises that there is a question of privilege which needs to be determined before the investigation or a prosecution can proceed.*

*Applications under the first two categories of this subhead have to be made within a set time period, as the question of privilege is known to exist and to ensure that the matter is raised and determined quickly. There is no time period where a production order has already been granted (the last category) as it could be some time before the question of privilege arises either because of the volume of data or otherwise.*

***Subhead (2)** is to allow a service provider (effectively a third party) who is the addressee of a production order to seek a determination as regards privilege.*

***Subhead (3)** deals with the situation where a preservation order or production order has been granted, and the person who is being investigated or the owner of the data wishes to raise the question of privilege. (Under Head 10 the data subject has to be advised of relevant preservation or production orders). No time period applies. It may be some time before they become aware of what data has been produced and have an opportunity to obtain legal advice. The subhead also applies to addressees such as a bank who are not service providers within the meaning of this scheme but may hold data on clients.*

***Subhead (4)** allows the High Court to make interim orders including to protect the data or to appoint an expert to review the data and advise the court on privilege. It follows the format of section 33(5) of the Competition and Consumer Protection Act 2014.*

***Subhead (5)** provides that once the question of privilege is to be determined, it must be on notice to the relevant parties, although the court has the power to order a heading to take place otherwise than in public to maintain the confidentiality of privileged material.*

***Subhead (6)** is intended to cover a situation where a judge has granted an indefinite preservation order under Head 6(5)(b) (or pursuant to Head 5) and the High Court has determined the matter of privilege. The onus is on the original applicant, an authorised person, to go back to the judge to have the preservation order discharged.*

## Head 6B - District Court jurisdictional provisions

(1) The following District Court judges shall have jurisdiction to hear and make decisions in respect of an application for a preservation order under Head 5 and for a production order under Head 6:

- A judge assigned to the District Court District in which the person, who has possession, control or lawful access to the data in question, resides or is located;
- A judge assigned to the District Court District in which there is located an establishment which has been designated or a legal representative appointed for the purposes of Article 1(1) and Article 3(1) of the Electronic Evidence Directive by the person, a service provider, who has possession, control or lawful access to the data in question;
- A judge assigned to the District Court District in which the offence or part of the offence was committed;
- A judge designated pursuant to Head 2A for the purposes of Part 2 of the Scheme.

(2)

(a) The person who is the controller of data within the meaning of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC shall be a person who has control of data for the purposes of this Head.

(b) In the case of a person who is a body corporate, their registered office in the State shall be regarded as the place where it resides for the purposes of this Head.

(3) A preservation order under Head 5 or a production order under Head 6 may only be issued in respect of data stored outside the jurisdiction of the State where:

- a person who has possession, control or lawful access to the data in question, resides or is located in the jurisdiction of the State or
- a person who is a service provider and who has possession, control or lawful access to the data in question has designated an establishment or appointed a legal representative located in the State for the purposes of Article 1(1) and Article 3(1) of the Electronic Evidence Directive.

(4) In this Head "Electronic Evidence Directive" means Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

## *Explanatory Notes*

***Subhead (1)*** *proposes a choice of grounds to establish jurisdiction for the District Court where applications may be made.*

- *The first is the District in which the person, who has possession, control or lawful access to the data in question, resides or is located. This basis for jurisdiction is in line with the requirements of Article 18 of the Budapest Convention to enable orders to be made in respect of a person in its territory in respect of "data in that person's possession or control".*

- *The second option arises from the Electronic Evidence Directive 2023/1544. This Directive forms part of the E-evidence Package along with the E-evidence Regulation to which this Bill relates. This Directive requires service providers providing a service within the EU to designate an establishment or legal representative within the EU to receive orders for the purpose of gathering electronic evidence, including domestic production orders made under national law. The second option provides that the District is linked to this designated recipient. The second option is being included to provide for an exceptional case where the first and third grounds for local jurisdiction would not apply - you might have a situation where a non-resident service provider designates a legal representative located in Ireland for the purposes of the Directive and the locus of the offence is not clear.*

- *The third option bases jurisdiction on where the offence was committed. This is a standard jurisdictional basis for the District Court in determining jurisdiction for a criminal trial.*

- *The fourth option is that of a designated special judge or judges. This may be appropriate if, in due course, the number and complexity of applications suggest greater specialisation is required and particularly if remote applications are facilitated.*

***Subhead (2)(a)*** *defines who is the data controller for the purposes of this Head with* ***Subhead 2(b)*** *explaining that if they are a body corporate, the location of their registered offices is where it "resides" for the purpose of this Head.*

***Subhead (3)*** *is intended to limit the District Court jurisdiction to grant domestic production or preservation order in respect of data stored outside the jurisdiction of the State to data relating to persons within the territory of the State*

***Subhead 4*** *provides a definition of "Electronic Evidence Directive".*

## Head 6C – Remote hearing of applications

(1) The President of the District Court may, of his or her own motion, on being satisfied that it is not contrary to the interests of justice direct that applications under Heads 5(2), 5(3), Head 6 (2), Head 6(3), Head 12(3) or Head 12(4) shall be heard using a live video link between the court and the place where the applicant is located.

(2) The District Court judge who is to hear the application, whether on application to it or of his or her own motion, make an order that the direction shall not apply in respect of a particular application on the grounds that a live video link is not available.

(3) The District Court judge hearing an application using a live video link in accordance with this Head and such video link fails or ceases to operate, may make such ancillary order or direction as he or she considers necessary in the interests of justice.

(4) Without prejudice to the power of the District Court judge hearing an application to make such provision in the absence of such rules, rules of court may make further provision to facilitate the hearing of an application to which this Head applies using a live video link between the court and the place where the applicant is located.

(5)

(a) Where an application is being made to which this Head applies, notwithstanding any provision in Head 5(4) or Head 6(4), such application shall be made
   (i) in electronic form,
   (ii) shall contain a statement that the person making the application has an honest belief that the facts stated therein are true,
   (iii) shall be signed by the person making it, entering his or her name in an electronic format or otherwise electronically as may be permitted by rules of court,
   (iv) shall be deemed to be an application made upon information on oath, and
   (v) shall comply with any other requirements as to its content, verification, authentication or form as may be prescribed by rules of court.

(b) Without prejudice to the law as to contempt of court, a person who makes or causes to be made, an application without an honest belief as to the truth of the matters in the application shall be guilty of an offence.

(c) A person guilty of an offence under paragraph (b) shall be liable
   (i) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 12 months or both:
   (ii) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years, or both.

(6) Where a preservation order or a production order is made pursuant to Head 5 or Head 6, a copy of that order shall be forwarded electronically to the applicant.

(7) This Head shall apply to applications made after a direction under subhead (1).

### *Explanatory Notes*

*The purpose of this Head is to facilitate the possibility of remote hearings of applications for preservation or production orders (including European Production Orders) in the future. This may prove to be the most efficient procedure for both the courts and applicants (particularly applicants from outside Dublin). However a number of administrative and procedural matters would have to be explored further before this Head could be commenced.*

*This Head is not intended to apply to applications under Head 6(8) to vary a production order as such applications will be in a full court hearing where both the applicant and the service provider/subject are likely to be present.*

## Head 7A - Amendment to Part 1 and the Schedule of the Criminal Justice (Mutual Assistance) Act 2008

(1) Section 2(1) of the Act of 2008 is amended :

(a) by the insertion of the following definition:
" '2001 Convention' means the Convention on Cybercrime done at Budapest on 23 November 2001;", and

(b) in the definition of "international instrument", by the insertion of the following paragraph after paragraph (l):

"(l.a) the 2001 convention".

(2) Section 2 (6) of the Act of 2008 is amended by the insertion of the following paragraph after paragraph (n):

"(o) Schedule 15 sets out the English text of the Convention on Cybercrime done at Budapest on 23 November 2001.".

(3) The Act of 2008 is amended by the insertion after Schedule 14 of Schedule 15 as set out in the Schedule to this Scheme.

### *Explanatory Notes*

*The purpose of this Head is to insert reference to the Budapest Convention in the Criminal Justice (Mutual Assistance) Act 2008 (the 2008 Act). This will ensure that states not previously covered by our mutual assistance regime via the 2008 Act and that subsequently become party to the Budapest Convention will automatically then be covered by our regime via the 2008 Act.*

## Head 7B – Amendment to section 75 of and insertion of section 75B in the Criminal Justice (Mutual Assistance) Act 2008

(1) Section 75 of the Act of 2008 is amended –

(a) by the insertion in subsection (1) of "or to make a production order or disclosure order" immediately before " in respect of an offence constituted by the conduct giving rise to the request.".

(b) in subsection (8):

(i) by the substitution of "sergeant" for "inspector", and

(ii) by the substitution of the following:

"**to the judge of the District Court for the district**
**(a) in which a person who has possession, control or lawful access to the material in question resides or is located or**
**(b) where the evidential material is situated,**
for an order under subsection (10)**."**

for

"to the judge of the District Court for the district where the evidential material is situated for an order under subsection (10).",

(c) in subsection (9) by the substitution of "believing that the person named in the request possesses, controls or has lawful access to the evidential material, the judge may make an order under subsection (10)." for "believing that the person named in the request possesses the evidential material, the judge may make an order under subsection (10).",

(d) in subsection (10) –

(i) by the substitution of the following for paragraph (a):

"(a) shall require any person who appears to the judge to be in possession of **or to have control of or to have lawful access to** the evidential material—
(i)to produce **or disclose** it to a named member of the Garda Síochána so that he or she may take it away, or
(ii)to give the member **and persons accompanying the member** access to it, either immediately or within a period specified in the order,",

(ii) by the substitution of the following for paragraph (b):

"(b) may, if the order relates to evidential material at any place and on application by a member of the Garda Síochána, require any person who appears to the judge

to be entitled to grant entry to the place to allow the member to enter it, **accompanied by such other members or persons or both as the member thinks necessary**, to obtain access to the material,"

(iii) in paragraph (c) to substitute

"shall authorise such a member if the person who is so required to grant entry to the place or to provide lawful access to the material does not do so—"

for

"shall authorise such a member, if the person who is so required to grant entry to the place does not do so—",

(iv) to substitute the following for subparagraph (iii) of (c):

"(iii) to access, examine, seize, take away and retain any evidential material which is found at the place **or in the possession of or in the control of or which can be lawfully accessed** by a person so present and which the member reasonably believes to be the material concerned, and",.

(e) to substitute the following for subsection (16)

"(16)

(a) A person who—

(i) obstructs or attempts to obstruct a member of the Garda Síochána acting under the authority of an order under this section,
(ii) fails to comply with a requirement in an order under this section, or
(iii) gives a false or misleading name or address to a member,

**is guilty of an offence under this section and shall be liable—**

**I. on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or**

**II. on conviction on indictment, to a fine not exceeding €500,000 or imprisonment for a term not exceeding 5 years or both.**

**(b) In proceedings for an offence under this subsection, it shall be a defence for a person against whom such proceedings are brought to prove that the person took all reasonable steps and exercised all due diligence to avoid the commission of the offence**. "

(f) to substitute the following for subsection (19):

"(19) In this section

**"data" has the same meaning as in the Act of 2017;**

["evidential material" includes any such material **or any data including** that relating to assets or proceeds deriving from criminal conduct in the designated state concerned or their identity or whereabouts;]

"member state" includes the Swiss Confederation.

(2) The following section shall be inserted in the Act of 2008 immediately after section 75A:

"75B Compliance with requests for material evidence subject to assurance

The Minister shall not proceed in accordance with a request pursuant to sections 63, 74 or 75 unless an assurance is given by the requesting authority that the material that may be furnished in response to the request may be challenged by the defendant at trial in the requesting state.**"**

## *Explanatory Notes*

*The purpose of this head is to ensure that the Criminal Justice (Mutual Assistance) Act 2008 Act (the 2008 Act) now covers mutual assistance in respect of the production/disclosure of data measures that will be introduced in this bill, and similar measures introduced via 2022 Act (amending the 2011 Act).*

*The 2008 Act envisages production of material on foot of a mutual legal assistance request where there is a corresponding domestic measure that would enable the production of the material on foot of a search warrant. Search warrants are tied to a geographic location and so are not suitable to retrieve data held in the cloud, unlike production/disclosure orders.*

***Subhead (1)(a)** is intended to make it clear that the provisions of section 75 of the 2008 Act may be applied to disclosure and productions orders.*

***Subhead (1)(b**) amends section 75(8) of the 2008 Act which currently requires an application for an order under the section to be made to a judge of the district where the evidential material is situated. As indicated above, this causes difficulties in respect of e-evidence where physical location is not appropriate. The amendment proposes to expand this so that an application can be made based on the location of a person who has possession, control or lawful access to the material in question (covers e-evidence) or, as at present, based on the physical location of the evidential material.*

*It also reduces the rank of Garda member who may apply from Inspector to Sergeant.*

***Subhead (1)(c)*** *is a minor amendment to subsection 75(9) to ensure consistency in the use of the term "possess, controls or has lawful access to" the evidential material in the 2008 Act.*

***Subhead (1)(d)*** *amends subhead 75(10) of the 2008 Act to reflect that a member of the Gardai giving effect to an order under section 75 may require expert assistance and it is permissible for them to be accompanied to facilitate this.*

***Subhead (1)(e)*** *amends subhead 75(16) - the offence provision - to match the penalties in Head 9.*

***Subhead (1)(f)*** *refers to the definition of "data" as used in the 2017 Act. The existing definition of data in section 75 specifies that "evidential material" includes any such material relating to assets or proceeds of crime. This amendment makes it clear that "evidential material" includes computer data.*

***Subhead (2)*** *provides for an assurance regarding the right of the accused to challenge evidence at the trial in the requesting state.*

## Head 8 – Amendments to the Criminal Justice (Offences Relating to Information Systems) Act 2017

(1) Section 1 of the Act of 2017 is amended by the substitution of the following for "'relevant offence' means an offence under section 2,3,4,5,6 or 9(1)":

> "'relevant offence' means an offence under section 2,3,4,5,6 or 9(1) of this Act, under Head 4 of the Criminal Justice (Protection, Preservation of and Access to Data on Information Systems) Bill 2024, under section 6,9 or 25 of the Criminal Justice(Theft and Fraud Offences) Act 2001, under section 5, 5A, or 6 of the Child Trafficking and Pornography Act 1998 as amended by the Criminal Law (Sexual Offences) Act 2017, under section 140 or 258 of the Copyright and Related Rights Act 2000.

(2) Subsections (3) and (4) of section 1 of the Act of 2017 is amended by the substitution of the following for those subsections:

"(3) The authority conferred by subsection (2)(c) to seize and retain anything includes, in the case of **data**, a document or record, authority—

(a) to make and retain a copy of the document or record,
(b) where necessary, to seize and, for long as is necessary, retain any computer in which any record is kept, and
(c) to render inaccessible or remove data from an information system where such data might facilitate the commission of an offence.

(4) A member acting under the authority of a search warrant under this section may—
(a) operate any computer at the place that is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and
(b) require any person at that place who appears to the member to have lawful access to the information in any such computer—

(i) to give to the member any password necessary to operate it and any encryption key or code necessary to unencrypt the information accessible by the computer,
(ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible,
(iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible, or
(iv) **to render inaccessible or remove data from an information system.**".

## *Explanatory Notes*

***Subhead (1)*** *extends the scope of relevant offences for the purposes of corporate liability, and search warrants and for asserting certain extra-territorial jurisdiction and related evidence and double jeopardy measures - as all originally provided for under the 2017 Act - to cybercrime-related offences included in the Budapest Convention.*

***Subhead (2)*** *extends search and seizure powers as provided for under the 2017 Act to rendering inaccessible or remove those computer data in the accessed computer system, a requirement of the Budapest Convention. A safeguard included is that this authority only applies where such data might facilitate the commission of an offence*

## Head 8A –Amendments to the Criminal Justice (Theft and Fraud Offences) Act 2001

Section 25 of the Criminal Justice (Theft and Fraud Offences) Act 2001 is amended by the insertion of the following after subsection (1):

"(1A) A person is guilty of [computer related] forgery if he or she inputs, alters, deletes or suppresses data in an information system or to be used in an information system 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.

(1B) For the purpose of this section "data" and "information system" shall have the same meaning as in the Criminal Justice (Offences Relating to Information Systems) Act 2017.".

### *Explanatory Notes*

*This Head inserts a new provision for an offence of computer related forgery into section 25 the Criminal Justice (Theft and Fraud Offences) Act 2001. This is a requirement of Article 7 of the Budapest Convention.*

## Head 9 – Offences

(1) A person who contravenes Head 5(11), Head 6 (6) or Head 6 (9) shall be guilty of an offence.

(2) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
(b) on conviction on indictment, to a fine not exceeding €500,000 or imprisonment for a term not exceeding 5 years or both.

(3) In proceedings for an offence under subsection (1), it shall be a defence for a person against whom such proceedings are brought to prove that the person took all reasonable steps and exercised all due diligence to avoid the commission of the offence.

(4) Where an offence under this section is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person being a director, manager, secretary or other officer of the body corporate or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.

### *Explanatory Notes*

*This Head is intended to provide for offences relating to non-compliance with preservation and productions orders.*

## Head 10 - Notification of data subject

(1) Subject to subsection (3), where data has been disclosed to a person pursuant to a requirement under Head 6, the applicant for that order shall cause to be given to the person to whom the data relates a notice in writing informing him or her of the disclosure of the data concerned
(2) Subject to subsection (3), where a preservation order has been made, the applicant for that preservation order, shall cause to be given to the person to whom the data relates a notice in writing informing him or her of the preservation of the data concerned
(3) The criteria set out in section 94 of the Data Protection Act 2018 shall apply in respect of any decision to postpone or otherwise restrict the notice provided for in subheads (1) and (2).

### *Explanatory Notes*

***Subhead (1)*** *provides for disclosure to the person whose data is subject to a production order, so that a person in due course will be aware their data has been accessed.*

***Subhead (2)*** *covers preservation orders and requires the data subject to be made aware of the preservation order as the data subject may wish to raise the question of privilege under Head 6A.*

***Subhead (3)*** *provides that section 94 of the Data Protection Act 2018 applies. This deals with the rights of and notice/disclosure obligations to data subjects and exceptions to this on proportionality grounds in a range of law enforcement contexts.*

## Head 11 - Service of documents

(1) A notice or other document that is required to be served on or given to a person under this Scheme shall be addressed to the person concerned by name and shall be so served on or given to the person—

(a) by electronic means,
(b) by delivering it to the person,
(c) by leaving it at the address at which the person ordinarily resides or carries on business or, in a case in which an address for service has been furnished, at that address,
(d) by sending it by post in a prepaid registered letter or by any other form of recorded delivery service to the address referred to in paragraph (c).

(2) For the purposes of this Head and subject to subhead (3), a company within the meaning of the Companies Act 2014 is deemed to be ordinarily resident at its registered office, and every other body corporate and every unincorporated body of persons shall be deemed to be ordinarily resident at its principal office or place of business.

(3) [Notwithstanding subhead (1)(c) or subhead (2), a service provider who has designated an establishment or appointed a legal representative in the State for the purposes of Article 1(1) and Article 3(1) of the Electronic Evidence Directive shall be deemed to be ordinarily resident at the establishment so designated or at the address of the legal representative for the purpose of this Head.

(4) In this Head "Electronic Evidence Directive" means Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.]

### *Explanatory Notes*

*This is a straightforward procedural provision regarding serving the documents on the addressee of an order.*

## Part 3 – European Preservation and Production Orders

Note: This Part is intended to facilitate compliance with article 31(1)(a) of Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings under which member states must notify to the Commission the authorities competent under national law to issue, validate or transmit European Production Orders or European Preservation Orders pursuant to article 4.

### Head 12 European Preservation and Production Orders

(1) Subject to the provisions of this Head and the EU Regulation, a designated judge shall be competent to issue a European Preservation Order or a European Production Order on application to him or her by an authorised person.

(2) Subject to the provisions of this Head and the EU Regulation, a designated judge shall be competent to issue a European Preservation Order or a European Production Order on application to him or her by or behalf a person charged with a serious offence subject to subhead (5).

(3) An application for a European Preservation Order pursuant to subsection (1) shall -

(a) be made ex parte,
(b) be upon information on oath specifying:

(i) the addressee of the European Preservation Order as referred to in Article 7 of EU Regulation;
(ii) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, login ID or account name;
(iii) details of data to be preserved including whether the data sought to be preserved is subscriber data, data requested for the sole purpose of identifying the user traffic data or content data;
(iv) if applicable, the time range requested to be preserved;
(v) the criminal offence to which it relates, or if it relates to the execution of a custodial sentence or detention order, details of the offence, conviction and sentence imposed;
(vi) the grounds for the necessity and proportionality of the measure, including why the data being sought to be preserved is regarded as vulnerable to removal, deletion or alteration;
(vii) reference to the provision in Irish law that would allow the issue of a Preservation Order in the comparable circumstances:
(viii) whether or not there is any reasonable indication that any of the data sought may be subject to privilege from disclosure in criminal proceedings under the law of the State or protected by immunities or privileges under the law of the enforcing State or that the data in question are covered by rules in the enforcing state on the determination and limitation of criminality relating to freedom of the press or freedom of expression in other media,

(c) be heard otherwise than in public.

(4) An application for a European Production Order pursuant to subsection (1) shall -

(a) be made ex parte,
(b) be upon information on oath specifying:
(i) the addressee of the European Production Order as referred to in Article 7 of eEvidence Regulation;
(ii) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, login ID or account name;
(iii) details of data sought including whether the data sought is subscriber data, data requested for the sole purpose of identifying the user traffic data or content data;
(iv) if applicable, the time range requested to be preserved;
(v) the criminal offence to which it relates, or if it relates to the execution of a custodial sentence or detention order, details of the offence, conviction and sentence imposed;
(vi) the grounds for the necessity and proportionality of the measure;
(vii) reference to the provision in Irish law that would allow the issue of a Production Order in the comparable circumstances;
(viii) a summary description of the case:
(ix) whether or not there is any reasonable indication that any of the data sought may be subject to privilege from disclosure in criminal proceedings under the law of the State or protected by immunities or privileges under the law of the enforcing State or that the data in question are covered by rules in the enforcing state on the determination and limitation of criminality relating to freedom of the press or freedom of expression in other media,

(c) be heard otherwise than in public.

(5) An application for a European Preservation Order pursuant to subsection (2) shall -

(a) be made on notice to the Director of Public Prosecutions,
(b) be upon information on oath specifying:

(i) the addressee of the European Preservation Order as referred to in Article 7 of eEvidence Regulation;
(ii) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, login ID or account name;
(iii) details of data to be preserved including whether the data sought to be preserved is subscriber data, data requested for the sole purpose of identifying the user traffic data or content data;
(iv) if applicable, the time range requested to be preserved;
(v) details of the criminal offence in respect of which the person has been charged and maximum penalty in respect of that offence;
(vi) the grounds for the necessity and proportionality of the measure, including why the data being sought to be preserved is regarded as vulnerable to removal, deletion or alteration;
(vii) reference to the provision in Irish law that would allow the issue of a Preservation Order for the same offence;

(viii) whether or not there is any reasonable indication that any of the data sought may be subject to privilege from disclosure in criminal proceedings under the law of the State or protected by immunities or privileges under the law of the enforcing State or that the data in question are covered by rules in the enforcing state on the determination and limitation of criminality relating to freedom of the press or freedom of expression in other media.

(6)

(a) A designated establishment or legal representative designated as an addressee in the State for the purposes the EU Directive who does not comply with a European Preservation Order or a European Production Order addressed to them shall be guilty of an offence.

(b) A person guilty of an offence under this subsection shall be liable—

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
(ii) on conviction on indictment, to a fine not exceeding €500,000 or imprisonment for a term not exceeding 5 years or both.

(c) In proceedings for an offence under paragraph (a), it shall be a defence for a person against whom such proceedings are brought to prove that the person took all reasonable steps and exercised all due diligence to avoid the commission of the offence.

(d) Where an offence under this section is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person being a director, manager, secretary or other officer of the body corporate or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.

(7)

(a) In this Head

"EU Regulation" means Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings adopted on 12 July 2023;

"EU Directive" means: Directive (EU) 2023/1544 of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointments of legal representatives for the purpose of gathering electronic evidence in criminal proceedings adopted on 12 July 2023

(b) A word or expression used in this Head and also in the EU Regulation, shall unless the contrary intention appears, have the same meaning in this Head as it does in the EU Regulation.

(8) [A provision is likely to be included on the procedures to be followed for a review of a European Production Order pursuant to Article 17 of the EU Regulation.]

## *Explanatory Notes*

***Subhead (1)*** *provides that the competent Irish authority to issue European Preservation and Production orders will be designated judge(s) of the District Court.*

***Subhead (2)*** *– provides that a European Production Order may also be requested by a suspected or accused. This is required by Article 1.2 of the E-evidence Regulation. Subhead (5) makes provision for a special procedure for this defence-based request.*

***Subhead (3)*** *sets out the procedure for applications for a European Preservation order.*

***Subhead (4)*** *sets out the procedure for applications for a European Production Order.*

***Subheads (5)*** *covers the procedure whereby a suspected or accused person can apply for a European Preservation or Production Order.*

***Subhead (6)*** *makes it an offence for an Irish addressee not to comply with a European Production or Preservation Order from another member state.*

***Subhead (7)*** *as these provisions are complementary to those in the E-evidence Regulation, the terminology in the E-evidence Regulation is used in certain parts and this subhead is intended to make that clear.*

***Subhead 8*** *Article 17 of E-evidence Regulation provides for a review procedure in the event of conflicting obligations.*

## Part 4 – Terrorist Content Online

Note: The topic does not relate directly to the Budapest Convention but the subject matter of the EU Terrorist Content Online Regulation (**EU Regulation (2021/784) on addressing the dissemination of terrorist content online)**, which relates to regulating access to certain online material, and so is of a similar nature dealing with a form of cyber abuse. It addresses amendments to the Online Safety and Media Regulation Act 2022 (No 41 of 2022) which will pave the way for the designation of "Coimisiún na Meán" as the competent authority under article 12(1)(d) of the Regulation which relates to the authority to impose penalties in respect of infringements pursuant to article 18.

### Head 13 - Amendments to the Online Safety and Media Regulation Act 2022 / Broadcasting Act 2009.

(1) Point (a) of Section 139ZG of Chapter 1 of Part 8B of the Broadcasting Act 2009 inserted by section 47 of the Online Safety and Media Regulation Act 2022 shall be deleted and replaced by the following:

"(a) 'contravention' means

(i) a failure to comply with section 46J, 46K, 46L, 46M(2) or (3), a media service code, a media service rule, section 46P(1) or (2), section 106(3), section 127(6), section 128B(1) or (2), any rules made under section 128C, an online safety code, section 159B(1) (or any rules made under section 159B(6)) or section 159C(1) (or any rules made under section 159C(3) or (6));

(ii) from the date that the Commission is designated as a competent authority pursuant to article 12 (1) (d) of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, an infringement of Article 3 (3) and (6), Article 4(2) and (7), Article 5 (1), (2), (3), (5) and (6), Articles 6, 7, 10 and 11, Article 14(5), Article 15(1) and Article 17 of that Regulation;".

(2) Subsection (4) of Section 139ZS of Chapter 3 of Part 8B of the Broadcasting Act 2009 inserted by section 47 of the Online Safety and Media Regulation Act 2022 shall be deleted and replaced by the following:

"(4)

(a) subject to paragraph (b), in deciding under subsection (1)(b) whether or not to impose an administrative financial sanction on a provider, the Commission shall have regard to the matters referred to in paragraphs (a), (b), (c), (d), (e), (g), (h), (i), (j) and (k) of section 139ZW(3),

(b) in the case of a contravention within the meaning of section 139ZG (a) (ii), when deciding whether to impose a penalty the Commission shall take into account all relevant circumstances, including:

(i) the nature, gravity and duration of the infringement;

(ii) whether the infringement was intentional or negligent;

(iii)previous infringements by the hosting service provider;

(iv) the financial strength of the hosting service provider;
(v) the level of cooperation of the hosting service provider with the competent authorities;
(vi) the nature and size of the hosting service provider, in particular whether it is a micro, small or medium-sized enterprise;
(vii) the degree of fault of the hosting service provider, taking into account the technical and organisational measures taken by the provider to comply with the requirements of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.".

(3) Subsection (1)(b) of Section 139ZW of Chapter 4 of Part 8B of the Broadcasting Act 2009 as inserted by section 47 of the Online Safety and Media Regulation Act 2022 shall be deleted and replaced by the following:

"(b) in the case of a provider that is not an individual, €20,000,000 or, if greater, 10 per cent of the relevant turnover of the provider in the financial year preceding the date of the decision under section 139ZS to impose the sanction,
(c) notwithstanding paragraphs (a) or (b) in the case of a contravention within the meaning of section 139ZG (a) (ii) €20,000,000 or, if greater, 4 per cent of the provider's global turnover of the proceeding business year.".

(4) Subsection (3) of Section 139ZW of Chapter 4 of Part 8B of the Broadcasting Act 2009 as inserted by section 47 of the Online Safety and Media Regulation Act 2022 is amended by the deletion of "The Commission" and its replacement by "Subject to subsection (3A), the Commission".

(5) Section 139ZW of Chapter 4 of Part 8B of the Broadcasting Act 2009 as inserted by section 47 of the Online Safety and Media Regulation Act 2022 is amended by the insertion of the following subsection (3A) immediately preceding subsection (4):

"(3A) In the case of a contravention within the meaning of section 139ZG (a) (ii), the Commission shall have regard to the following matters when determining the amount of the administrative financial sanction imposed under section 139ZS:
(a) the nature, gravity and duration of the infringement;
(b) whether the infringement was intentional or negligent;
(c) previous infringements by the hosting service provider;
(d) the financial strength of the hosting service provider;
(e) the level of cooperation of the hosting service provider with the competent authorities;
(f) the nature and size of the hosting service provider, in particular whether it is a micro, small or medium-sized enterprise;
(g) the degree of fault of the hosting service provider, taking into account the technical and organisational measures taken by the provider to comply with the requirements of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021on addressing the dissemination of terrorist content online;
(h) whether there has been a systematic or persistent failure to comply with obligations pursuant Article 3 (3) Regulation (EU) 2021/784 of the European

Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

Subsection (5) of this section shall not apply in respect in the case of a contravention within the meaning of section 139ZG (a) (ii).".

(6) The following Head shall be inserted immediately following section 139ZF of chapter 6 of Part 8A of the Broadcasting Act 2009 inserted by section 45 of the Online Safety and Media Regulation Act 2022:

"139ZFA. Power to require information relevant to the Terrorist Content Online

(1) The Commission may by notice in writing require the provider of a service which the Commission has reason to believe may be a hosting service provider, within the meaning of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, to provide the Commission with any information relating to the service that appears to the Commission to be relevant to the discharge of its functions as a competent authority under the aforesaid Regulation.
(2) A provider of a service who fails, without reasonable excuse, to comply with a notice under subsection (1) shall be guilty of a category 1 offence.".

## *Explanatory Notes*

***Subhead (1)*** *amends the definition of "contravention" in the Broadcasting Act 2009 (as amended by the Online Safety and Media Regulation Act 2022) to include infringements which are subject to penalties under the EU Terrorist Content Online Regulation (the TCO Regulation). This means that once formally designated as a competent authority, Coimisiún na Meán can use the mechanisms provided in the Bill for the investigation, determination and imposition of penalties for contraventions of the Terrorist Content Online Regulation.*

***Subhead (2)*** *provides that when considering whether there was an infringement of TCO Regulation that can attract sanction via the Broadcasting Act 2009 (as amended by the Online Safety and Media Regulation Act 2022), the considerations as laid out in article 18(2) of the TCO Regulation will effectively apply.*

***Subhead (3)*** *inserts a requirement of article 18(3) of the TCO Regulation that, in the case of systematic or persistent failures to comply with the TCO Regulation, "financial penalties of up to 4% of the hosting service provider's global turnover" should be available as a sanction.*

***Subheads (4)*** *distinguishes Coimisiún na Meán's considerations when imposing financial sanctions for infringements of the TCO Regulation from considerations it should take when*

*exercising its other financial sanctioning powers the Broadcasting Act 2009 (as amended by Online Safety and Media Regulation Act 2022)*

***Subhead (5)*** *outlines what Coimisiún na Meán should consider when imposing financial sanctions for infringements of the TCO Regulation as required by article 18(2) and article 18(3) of the TCO Regulation. It also makes clear that the prohibition on financial sanction where it would cause bankruptcy or cause a provider to cease trading (which applies in respect of their other sanctioning powers under the Broadcasting Act 2009) is not applicable where in respect of a sanction for infringement of the TCO Regulation.*

***Subhead (6)*** *provides Coimisiún na Mean with information gathering powers to carry out its functions in respect of the TCO Regulation.*

## Schedule

**"Schedule 15 sets out the English text of the Convention on Cybercrime done at Budapest on 23 November 2001**

---

**Chapter I – Use of terms**

**Article 1 – Definitions**

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 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.

**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.

**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.

**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.

**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 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.

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.

**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.

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.

Title 4 – Offences related to infringements of copyright and related rights

**Article 10 – Offences related to infringements of copyright and related rights**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such

conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other 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.

## Title 5 – Ancillary liability and sanctions

### Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

### 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.

**Section 2 – Procedural law**

Title 1 – Common provisions

**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**

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.

## Title 2 – Expedited preservation of stored computer data

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.

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.

## Title 3 – Production order

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;

cany other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

**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 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.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1Each 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.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

**Section 3 – Jurisdiction**

**Article 22 – Jurisdiction**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

A in its territory; or

B on board a ship flying the flag of that Party; or

C on board an aircraft registered under the laws of that Party; or

D by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5When 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.

## Chapter III – International co-operation

### Section 1 – General principles

#### Title 1 – General principles relating to international co-operation

**Article 23 – General principles relating to international co-operation**

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes 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.

#### Title 2 – Principles relating to extradition

**Article 24 – Extradition**

1a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, 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.

7a 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 that the details held on the register are correct at all times.

## Title 3 – General principles relating to mutual assistance

### 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 of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

**Article 26 – Spontaneous information**

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

**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.

2a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party

of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

**Article 28 – Confidentiality and limitation on use**

1When 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.

2The 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.

**Section 2 – Specific provisions**

Title 1 – Mutual assistance regarding provisional measures

**Article 29 – Expedited preservation of stored computer data**

1A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual

assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

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.

7 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.

2Disclosure 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.

Title 2 – Mutual assistance regarding investigative powers

**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.

**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 regarding the real-time collection of traffic data**

1The 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.

2Each 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.

**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.

Title 3 – 24/7 Network

**Article 35 – 24/7 Network**

1Each 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.

2a 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.

## Chapter IV – Final provisions

### Article 36 – Signature and entry into force

1This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

### Article 37 – Accession to the Convention

1After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

### Article 38 – Territorial application

1Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

### Article 39 – Effects of the Convention

1The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

–the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

–the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

–the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

**Article 40 – Declarations**

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 possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

**Article 41 – Federal clause**

1A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

**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.

**Article 43 – Status and withdrawal of reservations**

1A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

**Article 44 – Amendments**

1Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

**Article 45 – Settlement of disputes**

1The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

**Article 46 – Consultations of the Parties**

1The Parties shall, as appropriate, consult periodically with a view to facilitating:

athe effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

bthe exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

cconsideration of possible supplementation or amendment of the Convention.

2The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

**Article 47 – Denunciation**

1Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

**Article 48 – Notification**

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

aany signature;

bthe deposit of any instrument of ratification, acceptance, approval or accession;

cany date of entry into force of this Convention in accordance with Articles 36 and 37;

dany declaration made under Article 40 or reservation made in accordance with Article 42;

eany other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Source : Treaty Office on http://conventions.coe.int -.