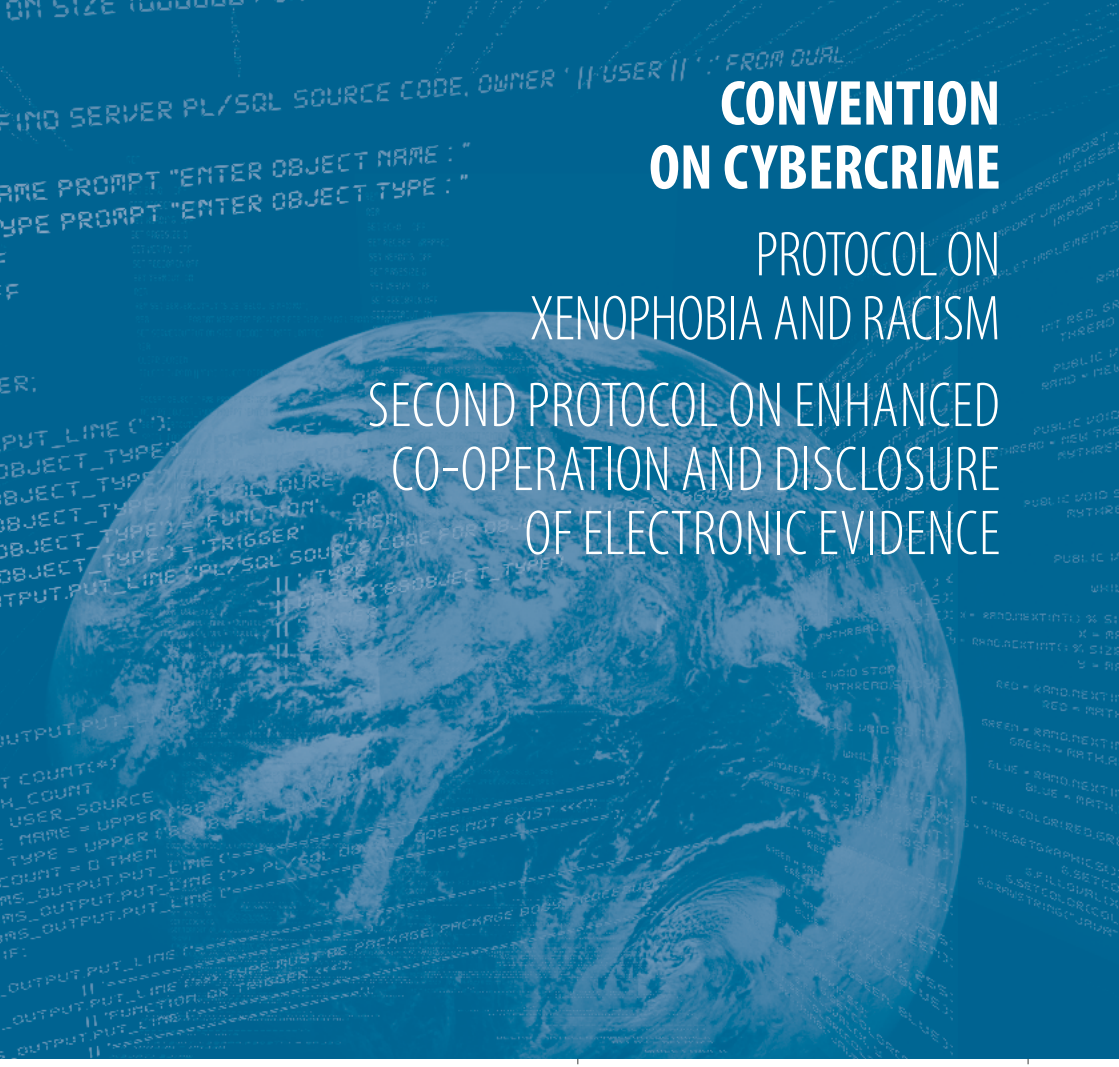

CONVENTION ON CYBERCRIME

PROTOCOL ON XENOPHOBIA AND RACISM

SECOND PROTOCOL ON ENHANCED CO-OPERATION AND DISCLOSURE OF ELECTRONIC EVIDENCE

Explanatory Reports
and Guidance Notes

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CONVENTION ON CYBERCRIME

PROTOCOL ON XENOPHOBIA AND RACISM

SECOND PROTOCOL ON ENHANCED CO-OPERATION AND DISCLOSURE OF ELECTRONIC EVIDENCE

Explanatory Reports and Guidance Notes

Council of Europe

Reproduction of the texts in this publication is authorised provided the full title and the source, namely the Council of Europe, are cited. If they are intended to be used for commercial purposes or translated into one of the non-official languages of the Council of Europe, please contact publishing@coe.int.

Cover and layout: Documents and Publications Production Department (DPDP), Council of Europe

© Council of Europe, January 2023
Printed at the Council of Europe

Contents

CONVENTION ON CYBERCRIME (ETS No.185)	**5**
Explanatory Report to the Convention on Cybercrime	35
FIRST ADDITIONAL PROTOCOL CONCERNING THE CRIMINALISATION OF ACTS OF A RACIST AND XENOPHOBIC NATURE COMMITTED THROUGH COMPUTER SYSTEMS (ETS No. 189), STRASBOURG, 28 JANUARY 2003	**131**
Explanatory Report to the First Additional Protocol	139
SECOND ADDITIONAL PROTOCOL ON ENHANCED CO-OPERATION AND DISCLOSURE OF ELECTRONIC EVIDENCE (ETS No. 224), STRASBOURG, 12 MAY 2022	**151**
Explanatory Report to the Second Additional Protocol	181
GUIDANCE NOTES	**281**
Guidance Note on the notion of "computer system"	282
Guidance Note on provisions of the Budapest Convention covering botnets	285
Guidance Note on DDOS attacks	289
Guidance Note on Identity theft and phishing in relation to fraud	291
Guidance Note on Critical information infrastructure attacks	296
Guidance Note on new forms of Malware	299
Guidance Note on Transborder access to data (Article 32)	302
Guidance Note Spam	309
Guidance Note on Production orders for subscriber information (Article 18 Budapest Convention)	312
Guidance Note on Terrorism	321
Guidance Note on Aspects of election interference by means of computer systems covered by the Budapest Convention	326
Guidance Note on Aspects of ransomware covered by the Budapest Convention	331

Convention on Cybercrime (ETS No.185)

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in 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 treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

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 the above Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

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;

c. any 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

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

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

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

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

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

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified

communications transmitted in its territory, through the application of technical means on that territory.

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

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

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.

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

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

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

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

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

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

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

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

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

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7.a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure 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.

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

b. The central authorities shall communicate directly with each other;

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

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

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

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

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

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

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

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

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject,

except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly 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

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

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

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

a. the authority seeking the preservation;

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

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

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

e. the necessity of the preservation; and

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

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to

a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this 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.

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

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

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

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 in the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their

territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

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

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a. the provision of technical advice;

b. the preservation of data pursuant to Articles 29 and 30;

c. the collection of evidence, the provision of legal information, and locating of suspects.

2.a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This 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.

2. This 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.

3. This 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.

4. In 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

1. After 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.

2. In 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

1. Any 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.

2. Any 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.

3. Any 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

1. The 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).

2. If 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.

3. Nothing 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

1. A 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.

2. When 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.

3. With 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

1. A 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.

2. A 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.

3. The 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

1. Amendments 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.

2. Any 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.

3. The 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.

4. The 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.

5. Any 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

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

2. In 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

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

a. the 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;

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

c. consideration of possible supplementation or amendment of the Convention.

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

3. The 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.

4. Except 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.

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

Article 47 – Denunciation

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

2. Such 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:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. any declaration made under Article 40 or reservation made in accordance with Article 42;

e. any 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.

Explanatory Report to the Convention on Cybercrime

I. The Convention and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001) and the Convention has been opened for signature in Budapest, on 23 November 2001, on the issue of the International Conference on Cyber-crime.

II. The text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions contained therein.

I. Introduction

1. The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalised their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities.

2. A conspicuous feature of information technology is the impact it has had and will have on the evolution of telecommunications technology. Classical telephony, involving the transmission of human voice, has been overtaken by the exchange of vast amounts of data, comprising voice, text, music and static and moving pictures. This exchange no longer occurs only between human beings, but also between human beings and computers, and between computers themselves. Circuit-switched connections have been replaced by packet-switched networks. It is no longer relevant whether a direct connection can be established; it suffices that data is entered into a network with a destination address or made available for anyone who wants to access it.

3. The pervasive use of electronic mail and the accessing through the Internet of numerous web sites are examples of these developments. They have changed our society profoundly.

4. The ease of accessibility and searchability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has lead to an explosive growth in the amount of information available and the knowledge that can be drawn there from.

5. These developments have given rise to an unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be more far- reaching than before because they are not restricted by geographical limitations or national boundaries. The recent spread of detrimental computer viruses all over the world has provided proof of this reality. Technical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour.

6. The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society.

II. The preparatory work

7. By decision CDPC/103/211196, the European Committee on Crime Problems (CDPC) decided in November 1996 to set up a committee of experts to deal with cyber-crime. The CDPC based its decision on the following rationale:

8. "The fast developments in the field of information technology have a direct bearing on all sections of modern society. The integration of telecommunication and information systems, enabling the storage and transmission, regardless of distance, of all kinds of communication opens a whole range of new possibilities. These developments were boosted by the emergence of information super-highways and networks, including the Internet, through which virtually anybody will be able to have access to any electronic information service irrespective of where in the world he is located. By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.

9. The criminal law must therefore keep abreast of these technological developments which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse. Whilst Recommendation No. (89) 9 resulted in the approximation of national concepts regarding certain forms of computer misuse, only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena. In the framework of such an instrument, in addition to measures of international co-operation, questions of substantive and procedural law, as well as matters that are closely connected with the use of information technology, should be addressed."

10. In addition, the CDPC took into account the Report, prepared – at its request – by Professor H.W.K. Kaspersen, which concluded that " … it should be looked to another legal instrument with more engagement than a Recommendation, such as a Convention. Such a Convention should not only deal with criminal substantive law matters, but also with criminal procedural questions as well as with international criminal law procedures and agreements."[1] A similar conclusion emerged already from the Report attached to Recommendation N° R (89) 9[2] concerning substantive law and from Recommendation N° R (95) 13[3] concerning problems of procedural law connected with information technology.

11. The new committee's specific terms of reference were as follows:

i. "Examine, in the light of Recommendations N° R (89) 9 on computer-related crime and N° R (95) 13 concerning problems of criminal procedural law connected with information technology, in particular the following subjects:

ii. cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;

---

1. Implementation of Recommendation N° R (89) 9 on computer-related crime, Report prepared by Professor Dr. H.W.K. Kaspersen (document CDPC (97) 5 and PC-CY (97) 5, page 106).
2. See Computer-related crime, Report by the European Committee on Crime Problems, page 86.
3. See Problems of criminal procedural law connected with information technology, Recommendation N° R (95) 13, principle n° 17.

iii. other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;

iv. the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, e.g. via the Internet, search and seizure in information-processing systems (including Internet sites), rendering illegal material inaccessible and requiring service providers to comply with special obligations, taking into account the problems caused by particular measures of information security, e.g. encryption;

v. the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (locus delicti) and which law should accordingly apply, including the problem of ne bis idem in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;

vi. questions of international co-operation in the investigation of cyber-space offences, in close co-operation with the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC).

The Committee should draft a binding legal instrument, as far as possible, on the items i) – v), with particular emphasis on international questions and, if appropriate, accessory recommendations regarding specific issues. The Committee may make suggestions on other issues in the light of technological developments."

12. Further to the CDPC's decision, the Committee of Ministers set up the new committee, called "the Committee of Experts on Crime in Cyber-space (PC-CY)" by decision n° CM/Del/Dec(97)583, taken at the 583rd meeting of the Ministers' Deputies (held on 4 February 1997). The Committee PC-CY started its work in April 1997 and undertook negotiations on a draft international convention on cyber-crime. Under its original terms of reference, the Committee was due to finish its work by 31 December 1999. Since by that time the Committee was not yet in a position to fully conclude its negotiations on certain issues in the draft Convention, its terms of reference were extended by decision n° CM/Del/Dec(99)679 of the Ministers' Deputies until 31 December 2000. The European Ministers of Justice expressed their support twice concerning the negotiations: by Resolution N° 1, adopted at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by

the CDPC on cyber-crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as by Resolution N° 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cyber-crime. The member States of the European Union expressed their support to the work of the PC-CY through a Joint Position, adopted in May 1999.

13. Between April 1997 and December 2000, the Committee PC-CY held 10 meetings in plenary and 15 meetings of its open-ended Drafting Group. Following the expiry of its extended terms of reference, the experts held, under the aegis of the CDPC, three more meetings to finalise the draft Explanatory Memorandum and review the draft Convention in the light of the opinion of the Parliamentary Assembly. The Assembly was requested by the Committee of Ministers in October 2000 to give an opinion on the draft Convention, which it adopted at the 2nd part of its plenary session in April 2001.

14. Following a decision taken by the Committee PC-CY, an early version of the draft Convention was declassified and released in April 2000, followed by subsequent drafts released after each plenary meeting, in order to enable the negotiating States to consult with all interested parties. This consultation process proved useful.

15. The revised and finalised draft Convention and its Explanatory Memorandum were submitted for approval to the CDPC at its 50th plenary session in June 2001, following which the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature.

III. The Convention

16. The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation.

17. The Convention, accordingly, contains four chapters: (I) Use of terms; (II) Measures to be taken at domestic level – substantive law and procedural law; (III) International co-operation; (IV) Final clauses.

18. Section 1 of Chapter II (substantive law issues) covers both criminalisation provisions and other connected provisions in the area of computer- or computer-related crime: it first defines 9 offences grouped in 4 different categories, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

19. Section 2 of Chapter II (procedural law issues) – the scope of which goes beyond the offences defined in Section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form – determines first the common conditions and safeguards, applicable to all procedural powers in this Chapter. It then sets out the following procedural powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data. Chapter II ends with the jurisdiction provisions.

20. Chapter III contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer- or computer-related crime specific assistance applies to both situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Parties.

21. Finally, Chapter IV contains the final clauses, which – with certain exceptions – repeat the standard provisions in Council of Europe treaties.

Commentary on the articles of the Convention

Chapter I – Use of terms

Introduction to the definitions at Article 1

22. It was understood by the drafters that under this Convention Parties would not be obliged to copy *verbatim* into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation.

Article 1 (a) – Computer system

23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

24. A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.

Article 1 (b) – Computer data

25. The definition of computer data builds upon the ISO-definition of data. This definition contains the terms "suitable for processing". This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion "computer data" is introduced. Computer data that is automatically processed may be the target of one of the criminal offences defined in this Convention as well as the object of the application of one of the investigative measures defined by this Convention.

Article 1 (c) – Service provider

26. The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems (cf. also comments on Section 2). Under (i) of the definition, it is made clear that both public and private entities which provide users the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether free of charge or for a fee. The closed group can be e.g. the employees of a private enterprise to whom the service is offered by a corporate network.

27. Under (ii) of the definition, it is made clear that the term "service provider" also extends to those entities that store or otherwise process data on behalf of the persons mentioned under (i). Further, the term includes those entities that store or otherwise process data on behalf of the users of the services of those mentioned under (i). For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his web site) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services.

Article 1 (d) – Traffic data

28. For the purposes of this Convention traffic data as defined in article 1, under subparagraph d., is a category of computer data that is subject to a specific legal regime. This data is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself.

29. In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive.

30. The definition lists exhaustively the categories of traffic data that are treated by a specific regime in this Convention: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. Not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

31. The definition leaves to national legislatures the ability to introduce differentiation in the legal protection of traffic data in accordance with its sensitivity. In this context, Article 15 obliges the Parties to provide for conditions and safeguards that are adequate for protection of human rights and liberties. This implies, *inter alia,* that the substantive criteria and the procedure to apply an investigative power may vary according to the sensitivity of the data.

Chapter II – Measures to be taken at the national level

32. Chapter II (Articles 2 – 22) contains three sections: substantive criminal law (Articles 2 – 13), procedural law (Articles 14 – 21) and jurisdiction (Article 22).

Section 1 – Substantive criminal law

33. The purpose of Section 1 of the Convention (Articles 2 – 13) is to improve the means to prevent and suppress computer or computer-related crime by

establishing a common minimum standard of relevant offences. This kind of harmonisation alleviates the fight against such crimes on the national and on the international level as well. Correspondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too. International co-operation (esp. extradition and mutual legal assistance) is facilitated e.g. regarding requirements of double criminality.

34. The list of offences included represents a minimum consensus not excluding extensions in domestic law. To a great extent it is based on the guidelines developed in connection with Recommendation No. R (89) 9 of the Council of Europe on computer-related crime and on the work of other public and private international organisations (OECD, UN, AIDP), but taking into account more modern experiences with abuses of expanding telecommunication networks.

35. The section is divided into five titles. Title 1 includes the core of computer-related offences, offences against the confidentiality, integrity and availability of computer data and systems, representing the basic threats, as identified in the discussions on computer and data security to which electronic data processing and communicating systems are exposed. The heading describes the type of crimes which are covered, that is the unauthorised access to and illicit tampering with systems, programmes or data. Titles 2 – 4 include other types of "computer-related offences", which play a greater role in practice and where computer and telecommunication systems are used as a means to attack certain legal interests which mostly are protected already by criminal law against attacks using traditional means. The Title 2 offences (computer-related fraud and forgery) have been added by following suggestions in the guidelines of the Council of Europe Recommendation No. R (89) 9. Title 3 covers the "content-related offences of unlawful production or distribution of child pornography by use of computer systems as one of the most dangerous *modi operandi* in recent times. The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the present Convention.

Title 4 sets out "offences related to infringements of copyright and related rights". This was included in the Convention because copyright infringements are one of the most widespread forms of computer- or computer-related crime and its escalation is causing international concern. Finally, Title 5 includes additional provisions on attempt, aiding and abetting and sanctions and measures, and, in compliance with recent international instruments, on corporate liability.

36. Although the substantive law provisions relate to offences using information technology, the Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.

37. The drafters of the Convention understood that Parties may exclude petty or insignificant misconduct from implementation of the offences defined in Articles 2-10.

38. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable *per se,* but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

39. All the offences contained in the Convention must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. For instance, in Article 8 on

computer-related fraud, the intent to procure an economic benefit is a constituent element of the offence. The drafters of the Convention agreed that the exact meaning of "intentionally" should be left to national interpretation.

40. Certain articles in the section allow the addition of qualifying circumstances when implementing the Convention in domestic law. In other instances even the possibility of a reservation is granted (cf. Articles 40 and 42). These different ways of a more restrictive approach in criminalisation reflect different assessments of the dangerousness of the behaviour involved or of the need to use criminal law as a countermeasure. This approach provides flexibility to governments and parliaments in determining their criminal policy in this area.

41. Laws establishing these offences should be drafted with as much clarity and specificity as possible, in order to provide adequate foreseeability of the type of conduct that will result in a criminal sanction.

42. In the course of the drafting process, the drafters considered the advisability of criminalising conduct other than those defined at Articles 2 – 11, including the so-called cyber-squatting, i.e. the fact of registering a domain-name which is identical either to the name of an entity that already exists and is usually well-known or to the trade-name or trademark of a product or company. Cyber-squatters have no intent to make an active use of the domain-name and seek to obtain a financial advantage by forcing the entity concerned, even though indirectly, to pay for the transfer of the ownership over the domain-name. At present this conduct is considered as a trademark-related issue. As trademark violations are not governed by this Convention, the drafters did not consider it appropriate to deal with the issue of criminalisation of such conduct.

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

43. The criminal offences defined under (Articles 2-6) are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.

Illegal access (Article 2)

44. "Illegal access" covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests

of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

45. The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above.

46. "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

47. The act must also be committed "without right". In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."

48. The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of "cookies" or "bots" to locate and retrieve information on behalf of communication. The application of such tools *per se* is not "without right". The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other

web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself "without right", in particular where the right holder of the accessed system can be considered to have accepted its application, e.g. in the case of "cookies" by not rejecting the initial instalment or not removing it.

49. Many national legislations already contain provisions on "hacking" offences, but the scope and constituent elements vary considerably. The broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the OECD Working Party in 1985.

50. Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extranets).

Illegal interception (Article 3)

51. This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights. The offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.

52. The text of the provision has been mainly taken from the offence of "unauthorised interception" contained in Recommendation (89) 9. In the

present Convention it has been made clear that the communications involved concern "transmissions of computer data" as well as electromagnetic radiation, under the circumstances as explained below.

53. Interception by "technical means" relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.

54. The offence applies to "non-public" transmissions of computer data. The term "non-public" qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. Therefore, the term "non-public" does not *per se* exclude communications via public networks. Communications of employees, whether or not for business purposes, which constitute "non-public transmissions of computer data" are also protected against interception without right under Article 3 (see e.g. ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92).

55. The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard). Nonetheless, Parties may require as an additional element that the communication be transmitted between computer systems remotely connected.

56. It should be noted that the fact that the notion of "computer system" may also encompass radio connections does not mean that a Party is under an obligation to criminalise the interception of any radio transmission which, even though "non-public", takes place in a relatively open and easily accessible manner and therefore can be intercepted, for example by radio amateurs.

57. The creation of an offence in relation to "electromagnetic emissions" will ensure a more comprehensive scope. Electromagnetic emissions may

be emitted by a computer during its operation. Such emissions are not considered as "data" according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision.

58. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities. It was also understood that the use of common commercial practices, such as employing "cookies", is not intended to be criminalised as such, as not being an interception "without right". With respect to non-public communications of employees protected under Article 3 (see above paragraph 54), domestic law may provide a ground for legitimate interception of such communications. Under Article 3, interception in such circumstances would be considered as undertaken "with right".

59. In some countries, interception may be closely related to the offence of unauthorised access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent, or that the offence be committed in relation to a computer system that is connected to another computer system in accordance with Article 2, may also require similar qualifying elements to attach criminal liability in this article. These elements should be interpreted and applied in conjunction with the other elements of the offence, such as "intentionally" and "without right".

Data interference (Article 4)

60. The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

61. In paragraph 1, "damaging" and "deteriorating" as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. "Deletion" of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable.

Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term "alteration" means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.

62. The above acts are only punishable if committed "without right". Common activities inherent in the design of networks or common operating or commercial practices, such as, for example, for the testing or protection of the security of a computer system authorised by the owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system acquires new software (e.g., software permitting access to the Internet that disables similar, previously installed programs), are with right and therefore are not criminalised by this article. The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right. However, Parties may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime.

63. In addition, the offender must have acted "intentionally".

64. Paragraph 2 allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation, but Parties should notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

System interference (Article 5)

65. This is referred to in Recommendation No. (89) 9 as computer sabotage. The provision aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The text is formulated in a neutral way so that all kinds of functions can be protected by it.

66. The term "hindering" refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data.

67. The hindering must furthermore be "serious" in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).

68. The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalised by this article, even if it causes serious hindering.

69. The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law.

70. The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

Misuse of devices (Article 6)

71. This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data. As the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2–5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries. A similar approach has already been taken in the 1929 Geneva Convention on currency counterfeiting.

72. Paragraph 1(a)1 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2-5 of the present Convention. "Distribution" refers to the active act of forwarding data to others, while "making available" refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a "computer program" refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

73. The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the

intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

74. Paragraph 1(a)2 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed.

75. Paragraph 1(b) creates the offence of possessing the items set out in paragraph 1(a)1 or 1(a)2. Parties are permitted, by the last phrase of paragraph 1(b), to require by law that a number of such items be possessed. The number of items possessed goes directly to proving criminal intent. It is up to each Party to decide the number of items required before criminal liability attaches.

76. The offence requires that it be committed intentionally and without right. In order to avoid the danger of overcriminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific (i.e. direct) intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention.

77. Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression "without right". For example, test-devices ("cracking-devices") and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be "with right".

78. Due to different assessments of the need to apply the offence of "Misuse of Devices" to all of the different kinds of computer offences in Articles 2 – 5, paragraph 3 allows, on the basis of a reservation (cf. Article 42), to restrict the offence in domestic law. Each Party is, however, obliged to criminalise at least the sale, distribution or making available of a computer password or access data as described in paragraph 1 (a) 2.

Title 2 – Computer-related offences

79. Articles 7 – 10 relate to ordinary crimes that are frequently committed through the use of a computer system. Most States already have criminalised these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones.

80. "Computer-related forgery" and "Computer-related fraud" deal with certain computer-related offences, i.e. computer-related forgery and computer-related fraud as two specific kinds of manipulation of computer systems or computer data. Their inclusion acknowledges the fact that in many countries certain traditional legal interests are not sufficiently protected against new forms of interference and attacks.

Computer-related forgery (Article 7)

81. The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations.

82. It should be noted that national concepts of forgery vary greatly. One concept is based on the authenticity as to the author of the document, and others are based on the truthfulness of the statement contained in the document. However, it was agreed that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term "authentic" the genuineness of the data.

83. This provision covers data which is the equivalent of a public or private document, which has legal effects. The unauthorised "input" of correct or incorrect data brings about a situation that corresponds to the making of a false document. Subsequent alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond in general to the falsification of a genuine document.

84. The term "for legal purposes" refers also to legal transactions and documents which are legally relevant.

85. The final sentence of the provision allows Parties, when implementing the offence in domestic law, to require in addition an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Computer-related fraud (Article 8)

86. With the arrival of the technological revolution the opportunities for committing economic crimes such as fraud, including credit card fraud, have multiplied. Assets represented or administered in computer systems (electronic funds, deposit money) have become the target of manipulations like traditional forms of property. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property.

87. To ensure that all possible relevant manipulations are covered, the constituent elements of "input", "alteration", "deletion" or "suppression" in Article 8(a) are supplemented by the general act of "interference with the functioning of a computer programme or system" in Article 8(b). The elements of "input, alteration, deletion or suppression" have the same meaning as in the previous articles. Article 8(b) covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.

88. The computer fraud manipulations are criminalised if they produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person. The term "loss of property", being a broad notion, includes loss of money, tangibles and intangibles with an economic value.

89. The offence must be committed "without right", and the economic benefit must be obtained without right. Of course, legitimate common commercial practices, which are intended to procure an economic benefit, are not meant to be included in the offence established by this article because they are conducted with right. For example, activities carried out pursuant to a valid contract between the affected persons are with right (e.g. disabling a web site as entitled pursuant to the terms of the contract).

90. The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit to another, but are not carried out with fraudulent or dishonest intent, are not meant to be included in the offence established by this article. For example, the use of information gathering programs to comparison shop on the Internet ("bots"), even if not authorised by a site visited by the "bot" is not intended to be criminalised.

Title 3 – Content-related offences

Offences related to child pornography (Article 9)

91. Article 9 on child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children.

92. This provision responds to the preoccupation of Heads of State and Government of the Council of Europe, expressed at their 2nd summit (Strasbourg, 10 – 11 October 1997) in their Action Plan (item III.4) and corresponds to an international trend that seeks to ban child pornography, as evidenced by the recent adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography (COM2000/854).

93. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most States already criminalise the traditional production and physical distribution of child pornography, but with the ever-increasing use of the Internet as the primary instrument

for trading such material, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children. It is widely believed that such material and on-line practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.

94. Paragraph 1(a) criminalises the production of child pornography for the purpose of distribution through a computer system. This provision was felt necessary to combat the dangers described above at their source.

95. Paragraph 1(b) criminalises the "offering" of child pornography through a computer system. "Offering" is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it. "Making available" is intended to cover the placing of child pornography on line for the use of others e.g. by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography.

96. Paragraph 1(c) criminalises the distribution or transmission of child pornography through a computer system. "Distribution" is the active dissemination of the material. Sending child pornography through a computer system to another person would be addressed by the offence of "transmitting" child pornography.

97. The term "procuring for oneself or for another" in paragraph 1(d) means actively obtaining child pornography, e.g. by downloading it.

98. The possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom, is criminalised in paragraph 1(e). The possession of child pornography stimulates demand for such material. An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession.

99. The term "pornographic material" in paragraph 2 is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt. Therefore, material having an artistic, medical, scientific or similar merit may be considered not to be pornographic. The visual depiction includes data stored on computer diskette or on other electronic means of storage, which are capable of conversion into a visual image.

100. A "sexually explicit conduct" covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated.

101. The three types of material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although "realistic", do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer.

102. In the three cases covered by paragraph 2, the protected legal interests are slightly different. Paragraph 2(a) focuses more directly on the protection against child abuse. Paragraphs 2(b) and 2(c) aim at providing protection against behaviour that, while not necessarily creating harm to the "child" depicted in the material, as there might not be a real child, might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favouring child abuse.

103. The term "without right" does not exclude legal defences, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Accordingly, the term "without right" allows a Party to take into account fundamental rights, such as freedom of thought, expression and privacy. In addition, a Party may provide a defence in respect of conduct related to "pornographic material" having an artistic, medical, scientific or similar merit. In relation to paragraph 2(b), the reference to "without right" could also allow, for example, that a Party may provide that a person is relieved of criminal responsibility if it is established that the person depicted is not a minor in the sense of this provision.

104. Paragraph 3 defines the term "minor" in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a "child" in the UN Convention on the Rights of the Child (Article 1). It was considered an important policy matter to set a uniform international standard regarding age. It should be noted that the age refers to the use of (real or fictitious) children as sexual objects, and is separate from the age of consent for

sexual relations. Nevertheless, recognising that certain States require a lower age-limit in national legislation regarding child pornography, the last phrase of paragraph 3 allows Parties to require a different age-limit, provided it is not less than 16 years.

105. This article lists different types of illicit acts related to child pornography which, as in Articles 2–8, Parties are obligated to criminalise if committed "intentionally." Under this standard, a person is not liable unless he has an intent to offer, make available, distribute, transmit, produce or possess child pornography. Parties may adopt a more specific standard (see, for example, applicable European Community law in relation to service provider liability), in which case that standard would govern. For example, liability may be imposed if there is "knowledge and control" over the information which is transmitted or stored. It is not sufficient, for example, that a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.

106. Paragraph 4 permits Parties to make reservations regarding paragraph 1(d) and (e), and paragraph 2(b) and (c). The right not to apply these sections of the provision may be made in part or in whole. Any such reservation should be declared to the Secretary General of the Council of Europe at the time of signature or when depositing the Party's instruments of ratification, acceptance, approval or accession, in accordance with Article 42.

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

Offences related to infringements of copyright and related rights (Article 10)

107. Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet, which cause concern both to copyright holders and those who work professionally with computer networks. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent. Such protected works include literary, photographic, musical, audiovisual and other works. The ease with which unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks made it necessary to include provisions on criminal law sanctions and enhance international co-operation in this field.

108. Each Party is obliged to criminalise wilful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale". Paragraph 1 provides for criminal sanctions against infringements of copyright by means of a computer system. Infringement of copyright is already an offence in almost all States. Paragraph 2 deals with the infringement of related rights by means of a computer system.

109. Infringement of both copyright and related rights is as defined under the law of each Party and pursuant to the obligations the Party has undertaken in respect of certain international instruments. While each Party is required to establish as criminal offences those infringements, the precise manner in which such infringements are defined under domestic law may vary from State to State. However, criminalisation obligations under the Convention do not cover intellectual property infringements other that those explicitly addressed in Article 10 and thus exclude patent or trademark-related violations.

110. With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are 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 (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention.

111. The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty had not entered into force at the time of concluding the present Convention. These treaties are nevertheless important as they significantly update the international protection for intellectual property (especially with regard to the new right of "making available" of protected material "on demand" over the Internet) and improve the means to fight violations of intellectual property rights worldwide. However it is understood that the infringements

of rights established by these treaties need not be criminalised under the present Convention until these treaties have entered into force with respect to a Party.

112. The obligation to criminalise infringements of copyright and related rights pursuant to obligations undertaken in international instruments does not extend to any moral rights conferred by the named instruments (such as in Article 6bis of the Bern Convention and in Article 5 of the WIPO Copyright Treaty).

113. Copyright and related rights offences must be committed "wilfully" for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term "wilfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement (Article 61), governing the obligation to criminalise copyright violations.

114. The provisions are intended to provide for criminal sanctions against infringements "on a commercial scale" and by means of a computer system. This is in line with Article 61 of the TRIPS Agreement which requires criminal sanctions in copyright matters only in the case of "piracy on a commercial scale". However, Parties may wish to go beyond the threshold of "commercial scale" and criminalise other types of copyright infringement as well.

115. The term "without right" has been omitted from the text of this article as redundant, since the term "infringement" already denotes use of the copyrighted material without authorisation. The absence of the term "without right" does not a contrario exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

116. Paragraph 3 allows Parties not to impose criminal liability under paragraphs 1 and 2 in "limited circumstances" (e.g. parallel imports, rental rights), as long as other effective remedies, including civil and/or administrative measures, are available. This provision essentially allows Parties a limited exemption from the obligation to impose criminal liability, provided that they do not derogate from obligations under Article 61 of the TRIPS Agreement, which is the minimum pre-existing criminalisation requirement.

117. This article shall in no way be interpreted to extend the protection granted to authors, film producers, performers, producers of phonograms, broadcasting organisations or other right holders to persons that do not meet the criteria for eligibility under domestic law or international agreement.

Title 5 – Ancillary liability and sanctions

Attempt and aiding or abetting (Article 11)

118. The purpose of this article is to establish additional offences related to attempt and aiding or abetting the commission of the offences defined in the Convention. As discussed further below, it is not required that a Party criminalise the attempt to commit each offence established in the Convention.

119. Paragraph 1 requires Parties to establish as criminal offences aiding or abetting the commission of any of the offences under Articles 2-10. Liability arises for aiding or abetting where the person who commits a crime established in the Convention is aided by another person who also intends that the crime be committed. For example, although the transmission of harmful content data or malicious code through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section. Thus, there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision.

120. With respect to paragraph 2 on attempt, some offences defined in the Convention, or elements of these offences, were considered to be conceptually difficult to attempt (for example, the elements of offering or making available of child pornog raphy). Moreover, some legal systems limit the offences for which the attempt is punished. Accordingly, it is only required that the attempt be criminalised with respect to offences established in accordance with Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c).

121. As with all the offences established in accordance with the Convention, attempt and aiding or abetting must be committed intentionally.

122. Paragraph 3 was added to address the difficulties Parties may have with paragraph 2, given the widely varying concepts in different legislations and despite the effort in paragraph 2 to exempt certain aspects from the provision on attempt. A Party may declare that it reserves the right not to apply paragraph 2 in part or in whole. This means that any Party making a reservation as to that provision will have no obligation to criminalise attempt at all, or may select the offences or parts of offences to which it will attach criminal sanctions in relation to attempt. The reservation aims at enabling the widest possible ratification of the Convention while permitting Parties to preserve some of their fundamental legal concepts.

Corporate liability (Article 12)

123. Article 12 deals with the liability of legal persons. It is consistent with the current legal trend to recognise corporate liability. It is intended to impose liability on corporations, associations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 also contemplates liability where such a leading person fails to supervise or control an employee or an agent of the legal person, where such failure facilitates the commission by that employee or agent of one of the offences established in the Convention.

124. Under paragraph 1, four conditions need to be met for liability to attach. First, one of the offences described in the Convention must have been committed. Second, the offence must have been committed for the benefit of the legal person. Third, a person who has a leading position must have committed the offence (including aiding and abetting). The term "person who has a leading position" refers to a natural person who has a high position in the organisation, such as a director. Fourth, the person who has a leading position must have acted on the basis of one of these powers – a power of representation or an authority to take decisions or to exercise control – which demonstrate that such a physical person acted within the scope of his or her authority to engage the liability of the legal person. In sum, paragraph 1 obligates Parties to have the ability to impose liability on the legal person only for offences committed by such leading persons.

125. In addition, Paragraph 2 obligates Parties to have the ability to impose liability upon a legal person where the crime is committed not by the leading person described in paragraph 1, but by another person acting under the legal person's authority, i.e., one of its employees or agents acting within the scope of their authority. The conditions that must be fulfilled before liability can attach are that (1) an offence has been committed by such an employee or agent of the legal person, (2) the offence has been committed for the benefit of the legal person; and (3) the commission of the offence has been made possible by the leading person having failed to supervise the employee or agent. In this context, failure to supervise should be interpreted to include failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the legal person. Such appropriate and reasonable measures could be determined by various factors, such as the type of the business, its size, the standards or the established business best practices, etc. This should not be interpreted as requiring a general surveillance regime over employee communications (see also

paragraph 54). A service provider does not incur liability by virtue of the fact that a crime was committed on its system by a customer, user or other third person, because the term "acting under its authority" applies exclusively to employees and agents acting within the scope of their authority.

126. Liability under this Article may be criminal, civil or administrative. Each Party has the flexibility to choose to provide for any or all of these forms of liability, in accordance with the legal principles of each Party, as long as it meets the criteria of Article 13, paragraph 2, that the sanction or measure be "effective, proportionate and dissuasive" and includes monetary sanctions.

127. Paragraph 4 clarifies that corporate liability does not exclude individual liability.

Sanctions and measures (Article 13)

128. This article is closely related to Articles 2-11, which define various computer- or computer-related crimes that should be made punishable under criminal law. In accordance with the obligations imposed by those articles, this provision obliges the Contracting Parties to draw consequences from the serious nature of these offences by providing for criminal sanctions that are "effective, proportionate and dissuasive" and, in the case of natural persons, include the possibility of imposing prison sentences.

129. Legal persons whose liability is to be established in accordance with Article 12 shall also be subject to sanctions that are "effective, proportionate and dissuasive", which can be criminal, administrative or civil in nature. Contracting Parties are compelled, under paragraph 2, to provide for the possibility of imposing monetary sanctions on legal persons.

130. The article leaves open the possibility of other sanctions or measures reflecting the seriousness of the offences, for example, measures could include injunction or forfeiture. It leaves to the Parties the discretionary power to create a system of criminal offences and sanctions that is compatible with their existing national legal systems.

Section 2 – Procedural law

131. The articles in this Section describe certain procedural measures to be taken at the national level for the purpose of criminal investigation of the offences established in Section 1, other criminal offences committed by means of a computer system and the collection of evidence in electronic form of a criminal offence. In accordance with Article 39, paragraph 3, nothing in the

Convention requires or invites a Party to establish powers or procedures other than those contained in this Convention, nor precludes a Party from doing so.

132. The technological revolution, which encompasses the "electronic highway" where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the sphere of criminal law and criminal procedure. The ever-expanding network of communications opens new doors for criminal activity in respect of both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. Equally, safeguards should also be adapted or developed to keep abreast of the new technological environment and new procedural powers.

133. One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation.

134. The Convention adapts traditional procedural measures, such as search and seizure, to the new technological environment. Additionally, new measures have been created, such as expedited preservation of data, in order to ensure that traditional measures of collection, such as search and seizure, remain effective in the volatile technological environment. As data in the new technological environment is not always static, but may be flowing in the process of communication, other traditional collection procedures relevant to telecommunications, such as real-time collection of traffic data and interception of content data, have also been adapted in order to permit the collection of electronic data that is in the process of communication. Some of these measures are set out in Council of Europe Recommendation No. R (95) 13 on problems of criminal procedural law connected with information technology.

135. All the provisions referred to in this Section aim at permitting the obtaining or collection of data for the purpose of specific criminal investigations or proceedings. The drafters of the present Convention discussed whether the Convention should impose an obligation for service providers to routinely collect and retain traffic data for a certain fixed period of time, but did not include any such obligation due to lack of consensus.

136. The procedures in general refer to all types of data, including three specific types of computer data (traffic data, content data and subscriber data), which may exist in two forms (stored or in the process of communication). Definitions of some of these terms are provided in Articles 1 and 18. The applicability of a procedure to a particular type or form of electronic data depends on the nature and form of the data and the nature of the procedure, as specifically described in each article.

137. In adapting traditional procedural laws to the new technological environment, the question of appropriate terminology arises in the provisions of this section. The options included maintaining traditional language ("search" and "seize"), using new and more technologically oriented computer terms ("access" and "copy"), as adopted in texts of other international fora on the subject (such as the G8 High Tech Crime Subgroup), or employing a compromise of mixed language ("search or similarly access", and "seize or similarly secure"). As there is a need to reflect the evolution of concepts in the electronic environment, as well as identify and maintain their traditional roots, the flexible approach of allowing States to use either the old notions of "search and seizure" or the new notions of "access and copying" is employed.

138. All the articles in the Section refer to "competent authorities" and the powers they shall be granted for the purposes of specific criminal investigations or proceedings. In certain countries, only judges have the power to order or authorise the collection or production of evidence, while in other countries prosecutors or other law enforcement officers are entrusted with the same or similar powers. Therefore, "competent authority" refers to a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

Title 1 – Common provisions

139. The Section begins with two provisions of a general nature that apply to all the articles relating to procedural law.

Scope of procedural provisions (Article 14)

140. Each State Party is obligated to adopt such legislative and other measures as may be necessary, in accordance with its domestic law and legal

framework, to establish the powers and procedures described in this Section for the purpose of "specific criminal investigations or proceedings."

141. Subject to two exceptions, each Party shall apply the powers and procedures established in accordance with this Section to: (i) criminal offences established in accordance with Section 1 of the Convention; (ii) other criminal offences committed by means of a computer system; and (iii) the collection of evidence in electronic form of a criminal offence. Thus, for the purpose of specific criminal investigations or proceedings, the powers and procedures referred to in this Section shall be applied to offences established in accordance with the Convention, to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence. This ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of the powers and procedures set out in this Section. It ensures an equivalent or parallel capability for the obtaining or collection of computer data as exists under traditional powers and procedures for non-electronic data. The Convention makes it explicit that Parties should incorporate into their laws the possibility that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted.

142. There are two exceptions to this scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law. Many States limit the power of interception of oral communications or telecommunications to a range of serious offences, in recognition of the privacy of oral communications and telecommunications and the intrusiveness of this investigative measure. Likewise, this Convention only requires Parties to establish interception powers and procedures in relation to content data of specified computer communications in respect of a range of serious offences to be determined by domestic law.

143. Second, a Party may reserve the right to apply the measures in Article 20 (real-time collection of traffic data) only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories is not more restricted than the range of offences to which it applies the interception measures referred to in Article 21. Some States consider the collection of traffic data as being equivalent to the collection of content data in terms of privacy and intrusiveness. The right of reservation would permit these States to limit the application of the measures to collect traffic data, in

real-time, to the same range of offences to which it applies the powers and procedures of real-time interception of content data. Many States, however, do not consider the interception of content data and the collection of traffic data to be equivalent in terms of privacy interests and degree of intrusiveness, as the collection of traffic data alone does not collect or disclose the content of the communication. As the real-time collection of traffic data can be very important in tracing the source or destination of computer communications (thus, assisting in identifying criminals), the Convention invites Parties that exercise the right of reservation to limit their reservation so as to enable the broadest application of the powers and procedures provided to collect, in real-time, traffic data.

144. Paragraph (b) provides a reservation for countries which, due to existing limitations in their domestic law at the time of the Convention's adoption, cannot intercept communications on computer systems operated for the benefit of a closed group of users and which do not use public communications networks nor are they connected with other computer systems. The term "closed group of users" refers, for example, to a set of users that is limited by association to the service provider, such as the employees of a company for which the company provides the ability to communicate amongst themselves using a computer network. The term "not connected with other computer systems" means that, at the time an order under Articles 20 or 21 would be issued, the system on which communications are being transmitted does not have a physical or logical connection to another computer network. The term "does not employ public communications networks" excludes systems that use public computer networks (including the Internet), public telephone networks or other public telecommunications facilities in transmitting communications, whether or not such use is apparent to the users.

Conditions and safeguards (Article 15)

145. The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be

provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments. These instruments include the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols Nos. 1, 4, 6, 7 and 12 (ETS Nos. 5,[4] 9, 46, 114, 117 and 177), in respect of European States that are Parties to them. It also includes other applicable human rights instruments in respect of States in other regions of the world (e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights) which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.

146. Another safeguard in the convention is that the powers and procedures shall "incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures. Also, the explicit

4. The text of the Convention had been amended according to the provisions of Protocol No. 3 (ETS No. 45), which entered into force on 21 September 1970, of Protocol No. 5 (ETS No. 55), which entered into force on 20 December 1971 and of Protocol No. 8 (ETS No. 118), which entered into force on 1 January 1990, and comprised also the text of Protocol No. 2 (ETS No. 44) which, in accordance with Article 5, paragraph 3 thereof, had been an integral part of the Convention since its entry into force on 21 September 1970. All provisions which had been amended or added by these Protocols are replaced by Protocol No. 11 (ETS No. 155), as from the date of its entry into force on 1 November 1998. As from that date, Protocol No. 9 (ETS No. 140), which entered into force on 1 October 1994, is repealed and Protocol No. 10 (ETS No. 146) has lost its purpose.

limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.

147. Without limiting the types of conditions and safeguards that could be applicable, the Convention requires specifically that such conditions and safeguards include, as appropriate in view of the nature of the power or procedure, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards. As stated in Paragraph 215, Parties should clearly apply conditions and safeguards such as these with respect to interception, given its intrusiveness. At the same time, for example, such safeguards need not apply equally to preservation. Other safeguards that should be addressed under domestic law include the right against self-incrimination, and legal privileges and specificity of individuals or places which are the object of the application of the measure.

148. With respect to the matters discussed in paragraph 3, of primary importance is consideration of the "public interest", in particular the interests of "the sound administration of justice". To the extent consistent with the public interest, Parties should consider other factors, such as the impact of the power or procedure on "the rights, responsibilities and legitimate interests" of third parties, including service providers, incurred as a result of the enforcement measures, and whether appropriate means can be taken to mitigate such impact. In sum, initial consideration is given to the sound administration of justice and other public interests (e.g. public safety and public health and other interests, including the interests of victims and the respect for private life). To the extent consistent with the public interest, consideration would ordinarily also be given to such issues as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under this Chapter, or protection of proprietary interests.

Title 2 – Expedited preservation of stored computer data

149. The measures in Articles 16 and 17 apply to stored data that has already been collected and retained by data-holders, such as service providers. They do not apply to the real-time collection and retention of future traffic data or to real-time access to the content of communications. These issues are addressed in Title 5.

150. The measures described in the articles operate only where computer data already exists and is currently being stored. For many reasons, computer data relevant for criminal investigations may not exist or no longer be stored. For example, accurate data may not have been collected and retained, or if collected was not maintained. Data protection laws may have affirmatively required the destruction of important data before anyone realised its significance for criminal proceedings. Sometimes there may be no business reason for the collection and retention of data, such as where customers pay a flat rate for services or the services are free. Article 16 and 17 do not address these problems.

151. "Data preservation" must be distinguished from "data retention". While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe.

152. Articles 16 and 17 refer only to data preservation, and not data retention. They do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities. The preservation measures apply to computer data that "has been stored by means of a computer system", which presupposes that the data already exists, has already been collected and is stored. Furthermore, as indicated in Article 14, all of the powers and procedures required to be established in Section 2 of the Convention are "for the purpose of specific criminal investigations or proceedings", which limits the application of the measures to an investigation in a particular case. Additionally, where a Party gives effect to preservation measures by means of an order, this order is in relation to "specified stored computer data in the person's possession or control" (paragraph 2). The articles, therefore, provide only for the power to require preservation of existing stored data, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings.

153. The obligation to ensure preservation of data is not intended to require Parties to restrict the offering or use of services that do not routinely collect and retain certain types of data, such as traffic or subscriber data, as part of their legitimate business practices. Neither does it require them to implement

new technical capabilities in order to do so, e.g. to preserve ephemeral data, which may be present on the system for such a brief period that it could not be reasonably preserved in response to a request or an order.

154. Some States have laws that require that certain types of data, such as personal data, held by particular types of holders must not be retained and must be deleted if there is no longer a business purpose for the retention of the data. In the European Union, the general principle is implemented by Directive 95/46/EC and, in the particular context of the telecommunications sector, Directive 97/66/EC. These directives establish the obligation to delete data as soon as its storage is no longer necessary. However, member States may adopt legislation to provide for exemptions when necessary for the purpose of the prevention, investigation or prosecution of criminal offences. These directives do not prevent member States of the European Union from establishing powers and procedures under their domestic law to preserve specified data for specific investigations.

155. Data preservation is for most countries an entirely new legal power or procedure in domestic law. It is an important new investigative tool in addressing computer and computer-related crime, especially crimes committed through the Internet. First, because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained. One method of preserving its integrity is for competent authorities to search or similarly access and seize or similarly secure the data. However, where the custodian of the data is trustworthy, such as a reputable business, the integrity of the data can be secured more quickly by means of an order to preserve the data. For legitimate businesses, a preservation order may also be less disruptive to its normal activities and reputation than the execution of a search and seizure of its premises. Second, computer and computer-related crimes are committed to a great extent as a result of the transmission of communications through the computer system. These communications may contain illegal content, such as child pornography, computer viruses or other instructions that cause interference with data or the proper functioning of the computer system, or evidence of the commission of other crimes, such as drug trafficking or fraud. Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data

regarding these past communications is required (see further explanation on the importance of traffic data below under Article 17). Third, where these communications contain illegal content or evidence of criminal activity and copies of such communications are retained by service providers, such as e-mail, the preservation of these communications is important in order to ensure that critical evidence is not lost. Obtaining copies of these past communications (e.g., stored e-mail that has been sent or received) can reveal evidence of criminality.

156. The power of expedited preservation of computer data is intended to address these problems. Parties are therefore required to introduce a power to order the preservation of specified computer data as a provisional measure, whereby data will be preserved for a period of time as long as necessary, up to a maximum of 90 days. A Party may provide for subsequent renewal of the order. This does not mean that the data is disclosed to law enforcement authorities at the time of preservation. For this to happen, an additional measure of disclosure or a search has to be ordered. With respect to disclosure to law enforcement of preserved data, see paragraphs 152 and 160.

157. It is also important that preservation measures exists at the national level in order to enable Parties to assist one another at the international level with expedited preservation of stored data located in their territory. This will help to ensure that critical data is not lost during often time-consuming traditional mutual legal assistance procedures that enable the requested Party to actually obtain the data and disclose it to the requesting Party.

Expedited preservation of stored computer data (Article 16)

158. Article 16 aims at ensuring that national competent authorities are able to order or similarly obtain the expedited preservation of specified stored computer-data in connection with a specific criminal investigation or proceeding.

159. "Preservation" requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. It requires that it be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be "frozen" (i.e. rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users. The person to whom the order is addressed may, depending on the exact specifications of the order, still access the data. The article does not specify how data should be preserved. It is left to each Party

to determine the appropriate manner of preservation and whether, in some appropriate cases, preservation of the data should also entail its "freezing".

160. The reference to "order or similarly obtain" is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor). In some States, preservation orders do not exist in their procedural law, and data can only be preserved and obtained through search and seizure or production order. Flexibility is intended by the use of the phrase "or otherwise obtain" to permit these States to implement this article by the use of these means. However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases.

161. The power to order or similarly obtain the expeditious preservation of specified computer data applies to any type of stored computer data. This can include any type of data that is specified in the order to be preserved. It can include, for example, business, health, personal or other records. The measures are to be established by Parties for use "in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification." This can include situations where the data is subject to a short period of retention, such as where there is a business policy to delete the data after a certain period of time or the data is ordinarily deleted when the storage medium is used to record other data. It can also refer to the nature of the custodian of the data or the insecure manner in which the data is stored. However, if the custodian were untrustworthy, it would be more secure to effect preservation by means of search and seizure, rather than by means of an order that could be disobeyed. A specific reference to "traffic data" is made in paragraph 1 in order to signal the provisions particular applicability to this type of data, which if collected and retained by a service provider, is usually held for only a short period of time. The reference to "traffic data" also provides a link between the measures in Article 16 and 17.

162. Paragraph 2 specifies that where a Party gives effect to preservation by means of an order, the order to preserve is in relation to "specified stored computer data in the person's possession or control". Thus, the stored data may actually be in the possession of the person or it may be stored elsewhere but subject to the control of this person. The person who receives the order is obliged "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable

the competent authorities to seek its disclosure." The domestic law of a Party should specify a maximum period of time for which data, subject to an order, must be preserved, and the order should specify the exact period of time that the specified data is to be preserved. The period of time should be as long as necessary, up to a maximum of 90 days, to permit the competent authorities to undertake other legal measures, such as search and seizure, or similar access or securing, or the issuance of a production order, to obtain the disclosure of the data. A Party may provide for subsequent renewal of the production order. In this context, reference should be made to Article 29, which concerns a mutual assistance request to obtain the expeditious preservation of data stored by means of a computer system. That article specifies that preservation effected in response to a mutual assistance request "shall be for a period not less than 60 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."

163. Paragraph 3 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This requires Parties to introduce confidentiality measures in respect of expedited preservation of stored data, and a time limit in respect of the period of confidentiality. This measure accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. For law enforcement authorities, the expedited preservation of data forms part of initial investigations and, therefore, covertness may be important at this stage. Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order that other persons do not attempt to tamper with or delete the data. For the person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that the preservation measure has been undertaken helps to protect the privacy of the data subject or other persons who may be mentioned or identified in that data.

164. In addition to the limitations set out above, the powers and procedures referred to in Article 16 are also subject to the conditions and safeguards provided in Articles 14 and 15.

Expedited preservation and partial disclosure of traffic data (Article 17)

165. This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service providers were involved in the transmission of specified communications. "Traffic data" is defined in Article 1.

166. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data (see discussion related to preservation, above).

167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

168. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service providers. The article does not specify the means by which this may be achieved, leaving it to domestic law to determine a means that is consistent with its legal and economic system.

One means to achieve expeditious preservation would be for competent authorities to serve expeditiously a separate preservation order on each service provider. Nevertheless, obtaining a series of separate orders can be unduly time consuming. A preferred alternative could be to obtain a single order, the scope of which however would apply to all service providers that were identified subsequently as being involved in the transmission of the specific communication. This comprehensive order could be served sequentially on each service provider identified. Other possible alternatives could involve the participation of service providers. For example, requiring a service provider that was served with an order to notify the next service provider in the chain of the existence and terms of the preservation order. This notice could, depending on domestic law, have the effect of either permitting the other service provider to preserve voluntarily the relevant traffic data, despite any obligations to delete it, or mandating the preservation of the relevant traffic data. The second service provider could similarly notify the next service provider in the chain.

169. As traffic data is not disclosed to law enforcement authorities upon service of a preservation order to a service provider (but only obtained or disclosed subsequently upon the taking of other legal measures), these authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted. The competent authorities should specify clearly the type of traffic data that is required to be disclosed. Receipt of this information would enable the competent authorities to determine whether to take preservation measures with respect to the other service providers. In this way, the investigating authorities can trace the communication back to its origin, or forward to its destination, and identify the perpetrator or perpetrators of the specific crime being investigated. The measures in this article are also subject to the limitations, conditions and safeguards provided in Articles 14 and 15.

Title 3 – Production order

Production order (Article 18)

170. Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored

computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations.

171. A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

172. The production order refers to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.

174. The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases.

175. A further consideration for Parties is the possible inclusion of measures concerning confidentiality. The provision does not contain a specific reference to confidentiality, in order to maintain the parallel with the non-electronic world where confidentiality is not imposed in general regarding production orders. However, in the electronic, particularly on-line, world a production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data. Confidentiality could be essential for the success of the investigation.

176. With respect to the modalities of production, Parties could establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order. This could include reference

to a time period within which disclosure must be made, or to form, such as that the data or information be provided in "plain text", on-line or on a paper print-out or on a diskette.

177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

178. In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address). Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.

179. Therefore, subscriber information includes various types of information about the use of a service and the user of that service. With respect to the use of the service, the term means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service. The term "technical provisions" includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centres or LANs (local area networks).

180. Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider. It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement. This latter information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment (on the basis of the information provided according to the service agreement or arrangement) can be instrumental to an investigation.

181. However, this article should not be understood as to impose an obligation on service providers to keep records of their subscribers, nor would it require service providers to ensure the correctness of such information. Thus, a service provider is not obliged to register identity information of users of so-called pre-paid cards for mobile telephone services. Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.

182. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorise Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining.

183. The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services.

Title 4 – Search and seizure of stored computer data

Search and seizure of stored computer data (Article 19)

184. This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence

with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data *per se* will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data.

185. In the traditional search environment concerning documents or records, a search involves gathering evidence that has been recorded or registered in the past in tangible form, such as ink on paper. The investigators search or inspect such recorded data, and seize or physically take away the tangible record. The gathering of data takes place during the period of the search and in respect of data that exists at that time. The precondition for obtaining legal authority to undertake a search is the existence of grounds to believe, as prescribed by domestic law and human rights safeguards, that such data exists in a particular location and will afford evidence of a specific criminal offence.

186. With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain. For example, the gathering of the data occurs during the period of the search and in respect of data that exists at that time. The preconditions for obtaining legal authority to undertake a search remain the same. The degree of belief required for obtaining legal authorisation to search is not any different whether the data is in tangible form or in electronic form. Likewise, the belief and the search are in respect of data that already exists and that will afford evidence of a specific offence.

187. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form, on a physical medium (e.g., diskette), before the tangible medium containing the copy can

be seized and taken away. In the latter two situations, where such copies of the data are made, a copy of the data remains in the computer system or storage device. Domestic law should provide for a power to make such copies. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations.

188. Paragraph 1 requires Parties to empower law enforcement authorities to access and search computer data, which is contained either within a computer system or part of it (such as a connected data storage device), or on an independent data storage medium (such as a CD-ROM or diskette). As the definition of "computer system" in article 1 refers to "any device or a group of inter-connected or related devices", paragraph 1 concerns the search of a computer system and its related components that can be considered together as forming one distinct computer system (e.g., a PC together with a printer and related storage devices, or a local area network). Sometimes data that is physically stored in another system or storage device can be legally accessed through the searched computer system by establishing a connection with other distinct computer systems. This situation, involving linkages with other computer systems by means of telecommunication networks within the same territory (e.g., wide area network or Internet), is addressed at paragraph 2.

189. Although search and seizure of a "computer-data storage medium in which computer data may be stored" (para graph 1 (b)) may be undertaken by use of traditional search powers, often the execution of a computer search requires both the search of the computer system and any related computer-data storage medium (e.g., diskettes) in the immediate vicinity of the computer system. Due to this relationship, a comprehensive legal authority is provided in paragraph 1 to encompass both situations.

190. Article 19 applies to stored computer data. In this respect, the question arises whether an unopened e-mail message waiting in the mailbox of an ISP until the addressee will download it to his or her computer system, has to be considered as stored computer data or as data in transfer. Under the law of some Parties, that e-mail message is part of a communication and therefore its

content can only be obtained by applying the power of interception, whereas other legal systems consider such message as stored data to which article 19 applies. Therefore, Parties should review their laws with respect to this issue to determine what is appropriate within their domestic legal systems.

191. Reference is made to the term "search or similarly access". The use of the traditional word "search" conveys the idea of the exercise of coercive power by the State, and indicates that the power referred to in this article is analogous to traditional search. "Search" means to seek, read, inspect or review data. It includes the notions of searching for data and searching of (examining) data. On the other hand, the word "access" has a neutral meaning, but it reflects more accurately computer terminology. Both terms are used in order to marry the traditional concepts with modern terminology.

192. The reference to "in its territory" is a reminder that this provision, as all the articles in this Section, concern only measures that are required to be taken at the national level.

193. Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be "in its territory".

194. The Convention does not prescribe how an extension of a search is to be permitted or undertaken. This is left to domestic law. Some examples of possible conditions are: empowering the judicial or other authority which authorised the computer search of a specific computer system, to authorise the extension of the search or similar access to a connected system if he or she has grounds to believe (to the degree required by national law and human rights safeguards) that the connected computer system may contain the specific data that is being sought; empowering the investigative authorities to extend an authorised search or similar access of a specific computer system to a connected computer system where there are similar grounds to believe that the specific data being sought is stored in the other computer system; or exercising search or similar access powers at both locations in a co-ordinated and expeditious manner. In all cases the data to be searched must be lawfully accessible from or available to the initial computer system.

195. This article does not address "transborder search and seizure", whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation.

196. Paragraph 3 addresses the issues of empowering competent authorities to seize or similarly secure computer data that has been searched or similarly accessed under paragraphs 1 or 2. This includes the power of seizure of computer hardware and computer-data storage media. In certain cases, for instance when data is stored in unique operating systems such that it cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. This may also be necessary when the data carrier has to be examined in order to retrieve from it older data which was overwritten but which has, nevertheless, left traces on the data carrier.

197. In this Convention, "seize" means to take away the physical medium upon which data or information is recorded, or to make and retain a copy of such data or information. "Seize" includes the use or seizure of programmes needed to access the data being seized. As well as using the traditional term "seize", the term "similarly secure" is included to reflect other means by which intangible data is removed, rendered inaccessible or its control is otherwise taken over in the computer environment. Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, "maintain the integrity of the data", or maintain the "chain of custody" of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data.

198. The rendering inaccessible of data can include encrypting the data or otherwise technologically denying anyone access to that data. This measure could usefully be applied in situations where danger or social harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography. The term "removal" is intended to express the idea that while the data is removed or rendered inaccessible, it is not destroyed, but continues to exist. The suspect is temporarily deprived of the data, but it can be returned following the outcome of the criminal investigation or proceedings.

199. Thus, seize or similarly secure data has two functions: 1) to gather evidence, such as by copying the data, or 2) to confiscate data, such as by copying the data and subsequently rendering the original version of the data inaccessible or by removing it. The seizure does not imply a final deletion of the seized data.

200. Paragraph 4 introduces a coercive measure to facilitate the search and seizure of computer data. It addresses the practical problem that it may be

difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted. This provision, therefore, allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure.

201. This power is not only of benefit to the investigating authorities. Without such co-operation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.

202. The information that can be ordered to be provided is that which is necessary to enable the undertaking of the search and seizure, or the similarly accessing or securing. The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable provision may include disclosing a password or other security measure to the investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such case, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities.

203. Under paragraph 5 of this article, the measures are subject to conditions and safeguards provided for under domestic law on the basis of Article 15 of this Convention. Such conditions may include provisions relating to the engagement and financial compensation of witnesses and experts.

204. The drafters discussed further in the frame of paragraph 5 if interested parties should be notified of the undertaking of a search procedure In the on-line world it may be less apparent that data has been searched and seized (copied) than that a seizure in the off-line world took place, where seized

objects will be physically missing. The laws of some Parties do not provide for an obligation to notify in the case of a traditional search. For the Convention to require notification in respect of a computer search would create a discrepancy in the laws of these Parties. On the other hand, some Parties may consider notification as an essential feature of the measure, in order to maintain the distinction between computer search of stored data (which is generally not intended to be a surreptitious measure) and interception of flowing data (which is a surreptitious measure, see Articles 20 and 21). The issue of notification, therefore, is left to be determined by domestic law. If Parties consider a system of mandatory notification of persons concerned, it should be borne in mind that such notification may prejudice the investigation. If such a risk exists, postponement of the notification should be considered.

Title 5 – Real-time collection of computer data

205. Articles 20 and 21 provide for the real-time collection of traffic data and the real-time interception of content data associated with specified communications transmitted by a computer system. The provisions address the real-time collection and real-time interception of such data by competent authorities, as well as their collection or interception by service providers. Obligations of confidentiality are also addressed.

206. Interception of telecommunications usually refers to traditional telecommunications networks. These networks can include cable infrastructures, whether wire or optical cable, as well as inter-connections with wireless networks, including mobile telephone systems and microwave transmission systems. Today, mobile communications are facilitated also by a system of special satellite networks. Computer networks may also consist of an independent fixed cable infrastructure, but are more frequently operated as a virtual network by connections made through telecommunication infrastructures, thus permitting the creation of computer networks or linkages of networks that are global in nature. The distinction between telecommunications and computer communications, and the distinctiveness between their infrastructures, is blurring with the convergence of telecommunication and information technologies. Thus, the definition of "computer system" in Article 1 does not restrict the manner by which the devices or group of devices may be interconnected. Articles 20 and 21, therefore, apply to specified communications transmitted by means of a computer system, which could include transmission of the communication through telecommunication networks before it is received by another computer system.

207. Articles 20 and 21 do not make a distinction between a publicly or a privately owned telecommunication or computer system or to the use of systems and communication services offered to the public or to closed user groups or private parties. The definition of "service provider" in Article 1 refers to public and private entities that provide to users of their services the ability to communicate by means of a computer system.

208. This Title governs the collection of evidence contained in currently generated communications, which are collected at the time of the communication (i.e., "real time"). The data are intangible in form (e.g., in the form of transmissions of voice or electronic impulses). The flow of the data is not significantly interfered with by the collection, and the communication reaches its intended recipient. Instead of a physical seizure of the data, a recording (i.e., a copy) is made of the data being communicated. The collection of this evidence takes place during a certain period of time. A legal authority to permit the collection is sought in respect of a future event (i.e., a future transmission of data).

209. The type of data that can be collected is of two types: traffic data and content data. "Traffic data" is defined in Article 1 d to mean any computer data relating to a communication made by means of a computer system, which is generated by the computer system and which formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size and duration or the type of service. "Content data" is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).

210. In many States, a distinction is made between the real-time interception of content data and real-time collection of traffic data in terms of both the legal prerequisites required to authorise such investigative measure and the offences in respect of which this measure can be employed. While recognising that both types of data may have associated privacy interests, many States consider that the privacy interests in respect of content data are greater due to the nature of the communication content or message. Greater limitations may be imposed with respect to the real-time collection of content data than traffic data. To assist in recognising this distinction for these States, the Convention, while operationally acknowledging that the data is collected or recorded in both situations, refers normatively in the titles of the articles to the collection of traffic data as "real-time collection" and the collection of content data as "real-time interception".

211. In some States existing legislation makes no distinction between the collection of traffic data and the interception of content data, either because no distinction has been made in the law regarding differences in privacy interests or the technological collection techniques for both measures are very similar. Thus, the legal prerequisites required to authorise the undertaking of the measures, and the offences in respect of which the measures can be employed, are the same. This situation is also recognised in the Convention by the common operational use of the term "collect or record" in the actual text of both Articles 20 and 21.

212. With respect to the real-time interception of content data, the law often prescribes that the measure is only available in relation to the investigation of serious offences or categories of serious offences. These offences are identified in domestic law as serious for this purpose often by being named in a list of applicable offences or by being included in this category by reference to a certain maximum sentence of incarceration that is applicable to the offence. Therefore, with respect to the interception of content data, Article 21 specifically provides that Parties are only required to establish the measure "in relation to a range of serious offences to be determined by domestic law".

213. Article 20, concerning the collection of traffic data, on the other hand, is not so limited and in principle applies to any criminal offence covered by the Convention. However, Article 14, paragraph 3, provides that a Party may reserve the right to apply the measure only to offences or categories of offences specified in the reservation, provided that the range of offences or categories of offences is not more restricted than the range of offences to which it applies the measure of interception of content data. Nevertheless, where such a reservation is taken, the Party shall consider restricting such reservation so as to enable the broadest range of application of the measure of collection of traffic data.

214. For some States, the offences established in the Convention would normally not be considered serious enough to permit interception of content data or, in some cases, even the collection of traffic data. Nevertheless, such techniques are often crucial for the investigation of some of the offences established in the Convention, such as those involving illegal access to computer systems, and distribution of viruses and child pornography. The source of the intrusion or distribution, for example, cannot be determined in some cases without real-time collection of traffic data. In some cases, the nature of the communication cannot be discovered without real-time interception of content data. These offences, by their nature or the means of transmission,

involve the use of computer technologies. The use of technological means should, therefore, be permitted to investigate these offences. However, due to the sensitivities surrounding the issue of interception of content data, the Convention leaves the scope of this measure to be determined by domestic law. As some countries legally assimilate the collection of traffic data with the interception of content data, a reservation possibility is permitted to restrict the applicability of the former measure, but not to an extent greater than a Party restricts the measure of real-time interception of content data. Nevertheless, Parties should consider applying the two measures to the offences established by the Convention in Section 1 of Chapter II, in order to provide an effective means for the investigation of these computer offences and computer-related offences.

215. The conditions and safeguards regarding the powers and procedures related to real-time interception of content data and real-time collection of traffic data are subject to Articles 14 and 15. As interception of content data is a very intrusive measure on private life, stringent safeguards are required to ensure an appropriate balance between the interests of justice and the fundamental rights of the individual. In the area of interception, the present Convention itself does not set out specific safeguards other than limiting authorisation of interception of content data to investigations into serious criminal offences as defined in domestic law. Nevertheless, the following important conditions and safeguards in this area, applied in domestic laws, are: judicial or other independent supervision; specificity as to the communications or persons to be intercepted; necessity, subsidiarity and proportionality (e.g. legal predicates justifying the taking of the measure; other less intrusive measures not effective); limitation on the duration of interception; right of redress. Many of these safeguards reflect the European Convention on Human Rights and its subsequent case-law (see judgements in Klass,[5] Kruslin,[6] Huvig,[7] Malone,[8] Halford,[9] Lambert[10] cases). Some of these safeguards are applicable also to the collection of traffic data in real-time.

5. ECHR Judgment in the case of Klass and others v. Germany, A28, 06/09/1978.
6. ECHR Judgment in the case of Kruslin v. France, 176-A, 24/04/1990.
7. ECHR Judgment in the case of Huvig v. France, 176-B, 24/04/1990.
8. ECHR Judgment in the case of Malone v. United Kingdom, A82, 02/08/1984.
9. ECHR Judgment in the case of Halford v. United Kingdom, Reports 1997 – III, 25/06/1997.
10. ECHR Judgment in the case of Lambert v. France, Reports 1998 – V, 24/08/1998.

Real-time collection of traffic data (Article 20)

216. Often, historical traffic data may no longer be available or it may not be relevant as the intruder has changed the route of communication. Therefore, the real-time collection of traffic data is an important investigative measure. Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings.

217. Traditionally, the collection of traffic data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine the source or destination (e.g., telephone numbers) and related data (e.g., time, date and duration) of various types of illegal communications (e.g., criminal threats and harassment, criminal conspiracy, fraudulent misrepresentations) and of communications affording evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.).

218. Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it also has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography). Likewise, as computers can store vast quantities of data, often of a private nature, the potential for harm, whether economic, social or personal, can be significant if the integrity of this data is interfered with. Furthermore, as the science of computer technology is founded upon the processing of data, both as an end product and as part of its operational function (e.g., execution of computer programs), any interference with this data can have disastrous effects on the proper operation of computer systems. When an illegal distribution of child pornography, illegal access to a computer system or interference with the proper functioning of the computer system or the integrity of data, is committed, particularly from a distance such as through the Internet, it is necessary and crucial to trace the route of the communications back from the victim to the perpetrator. Therefore, the ability to collect traffic data in respect of computer communications is just as, if not more, important as it is in respect of purely traditional telecommunications. This investigative technique can correlate the time, date and source and destination of the suspect's communications with the time of the intrusions into the systems of victims, identify other victims or show links with associates.

219. Under this article, the traffic data concerned must be associated with specified communications in the territory of the Party. The specified "communications" are in the plural, as traffic data in respect of several communications

may need to be collected in order to determine the human source or destination (for example, in a household where several different persons have the use of the same telecommunications facilities, it may be necessary to correlate several communications with the individuals' opportunity to use the computer system). The communications in respect of which the traffic data may be collected or recorded, however, must be specified. Thus, the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of "fishing expeditions" where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.

220. Subject to paragraph 2, Parties are obliged, under paragraph 1(a) to ensure that their competent authorities have the capacity to collect or record traffic data by technical means. The article does not specify technologically how the collection is to be undertaken, and no obligations in technical terms are defined.

221. In addition, under paragraph 1(b), Parties are obliged to ensure that their competent authorities have the power to compel a service provider to collect or record traffic data or to co-operate and assist the competent authorities in the collection or recording of such data. This obligation regarding service providers is applicable only to the extent that the collection or recording, or co-operation and assistance, is within the existing technical capability of the service provider. The article does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems. However, if their systems and personnel have the existing technical capability to provide such collection, recording, co-operation or assistance, the article would require them to take the necessary measures to engage such capability. For example, the system may be configured in such a manner, or computer programs may already be possessed by the service provider, which would permit such measures to be taken, but they are not ordinarily executed or used in the normal course of the service provider's operation. The article would require the service provider to engage or turn-on these features, as required by law.

222. As this is a measure to be carried out at national level, the measures are applied to the collection or recording of specified communications in the territory of the Party. Thus, in practical terms, the obligations are generally applicable where the service provider has some physical infrastructure or

equipment on that territory capable of undertaking the measures, although this need not be the location of its main operations or headquarters. For the purposes of this Convention, it is understood that a communication is in a Party's territory if one of the communicating parties (human beings or computers) is located in the territory or if the computer or telecommunication equipment through which the communication passes is located on the territory.

223. In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a)). Likewise, an obligation under paragraph 1(b)(ii) to co-operate and assist the competent authorities in the collection or recording of traffic data is senseless if the competent authorities are not empowered to collect or record themselves the traffic data. Additionally, in the situation of some local area networks (LANs), where no service provider may be involved, the only way for collection or recording to be carried out would be for the investigating authorities to do it themselves. Both measures in paragraphs 1 (a) and (b) do not have to be used each time, but the availability of both methods is required by the article.

224. This dual obligation, however, posed difficulties for certain States in which the law enforcement authorities were only able to intercept data in telecommunication systems through the assistance of a service provider, or not surreptitiously without at least the knowledge of the service provider. For this reason, paragraph 2 accommodates such a situation. 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 a different approach, such as only compelling service providers to provide the necessary technical facilities, to ensure the real-time collection of traffic data by law enforcement authorities. In such case, all of the other limitations regarding territory, specificity of communications and use of technical means still apply.

225. Like real-time interception of content data, real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Interception is surreptitious and must be carried out in such a manner that the communicating parties will not perceive the operation. Service providers and their employees knowing about the interception must, therefore, be under an obligation of secrecy in order for the procedure to be undertaken effectively.

226. Paragraph 3 obligates Parties to adopt such legislative or other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data. This provision not only ensures the confidentiality of the investigation, but it also relieves the service provider of any contractual or other legal obligations to notify subscribers that data about them is being collected. Paragraph 3 may be effected by the creation of explicit obligations in the law. On the other hand, a Party may be able to ensure the confidentiality of the measure on the basis of other domestic legal provisions, such as the power to prosecute for obstruction of justice those persons who aid the criminals by telling them about the measure. Although a specific confidentiality requirement (with effective sanction in case of a breach) is a preferred procedure, the use of obstruction of justice offences can be an alternative means to prevent inappropriate disclosure and, therefore, also suffices to implement this paragraph. Where explicit obligations of confidentiality are created, these shall be subject to the conditions and safeguards as provided in Articles 14 and 15. These safeguards or conditions should impose reasonable time periods for the duration of the obligation, given the surreptitious nature of the investigative measure.

227. As noted above, the privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures, pursuant to Articles 14 and 15.

Interception of content data (Article 21)

228. Traditionally, the collection of content data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine that the communication is of an illegal nature (e.g., the communication constitutes a criminal threat or harassment, a criminal conspiracy or fraudulent misrepresentations) and to collect evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.). Computer communications can constitute or afford evidence of the same types of criminality.

However, given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography). Many of the computer crimes involve the transmission or communication of data as part of their commission; for example, communications sent to effect an illegal access of a computer system or the distribution of computer viruses. It is not possible to determine in real-time the harmful and illegal nature of these communications without intercepting the content of the message. Without the ability to determine and prevent the occurrence of criminality in progress, law enforcement would merely be left with investigating past and completed crimes where the damage has already occurred. Therefore, the real-time interception of content data of computer communications is just as, if not more, important as is the real-time interception of telecommunications.

229. "Content data" refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication. It is everything transmitted as part of the communication that is not traffic data.

230. Most of the elements of this article are identical to those of Article 20. Therefore, the comments, above, concerning the collection or recording of traffic data, obligations to co-operate and assist, and obligations of confidentiality apply equally to the interception of content data. Due to the higher privacy interest associated with content data, the investigative measure is restricted to "a range of serious offences to be determined by domestic law".

231. Also, as set forth in the comments above on Article 20, the conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data, or to the search and seizure or similar accessing or securing of stored data.

Section 3 – Jurisdiction

Jurisdiction (Article 22)

232. This Article establishes a series of criteria under which Contracting Parties are obliged to establish jurisdiction over the criminal offences enumerated in Articles 2-11 of the Convention.

233. Paragraph 1 *littera a* is based upon the principle of territoriality. Each Party is required to punish the commission of crimes established in this

Convention that are committed in its territory. For example, a Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not.

234. Consideration was given to including a provision requiring each Party to establish jurisdiction over offences involving satellites registered in its name. The drafters decided that such a provision was unnecessary since unlawful communications involving satellites will invariably originate from and/or be received on earth. As such, one of the bases for a Party's jurisdiction set forth in paragraph 1(a) – (c) will be available if the transmission originates or terminates in one of the locations specified therein. Further, to the extent the offence involving a satellite communication is committed by a Party's national outside the territorial jurisdiction of any State, there will be a jurisdictional basis under paragraph 1(d). Finally, the drafters questioned whether registration was an appropriate basis for asserting criminal jurisdiction since in many cases there would be no meaningful nexus between the offence committed and the State of registry because a satellite serves as a mere conduit for a transmission.

235. Paragraph 1, *litterae b* and *c* are based upon a variant of the principle of territoriality. These *litterae* require each Party to establish criminal jurisdiction over offences committed upon ships flying its flag or aircraft registered under its laws. This obligation is already implemented as a general matter in the laws of many States, since such ships and aircraft are frequently considered to be an extension of the territory of the State. This type of jurisdiction is most useful where the ship or aircraft is not located in its territory at the time of the commission of the crime, as a result of which Paragraph 1, *littera a* would not be available as a basis to assert jurisdiction. If the crime is committed on a ship or aircraft that is beyond the territory of the flag Party, there may be no other State that would be able to exercise jurisdiction barring this requirement. In addition, if a crime is committed aboard a ship or aircraft which is merely passing through the waters or airspace of another State, the latter State may face significant practical impediments to the exercise of its jurisdiction, and it is therefore useful for the State of registry to also have jurisdiction.

236. Paragraph 1, *littera d* is based upon the principle of nationality. The nationality theory is most frequently applied by States applying the civil law tradition. It provides that nationals of a State are obliged to comply with the domestic law even when they are outside its territory. Under *littera d,* if a national commits an offence abroad, the Party is obliged to have the ability

to prosecute it if the conduct is also an offence under the law of the State in which it was committed or the conduct has taken place outside the territorial jurisdiction of any State.

237. Paragraph 2 allows Parties to enter a reservation to the jurisdiction grounds laid down in paragraph 1, *litterae b, c,* and *d*. However, no reservation is permitted with respect to the establishment of territorial jurisdiction under *littera a,* or with respect to the obligation to establish jurisdiction in cases falling under the principle of *"aut dedere aut judicare"* (extradite or prosecute) under paragraph 3, i.e. where that Party has refused to extradite the alleged offender on the basis of his nationality and the offender is present on its territory. Jurisdiction established on the basis of paragraph 3 is necessary to ensure that those Parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if sought by the Party that requested extradition pursuant to the requirements of "Extradition", Article 24, paragraph 6 of this Convention.

238. The bases of jurisdiction set forth in paragraph 1 are not the exclusive. Paragraph 4 of this article permits the Parties to establish, in conformity with their domestic law, other types of criminal jurisdiction as well.

239. In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in many States. In order to avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings, the affected Parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph. Finally, the obligation to consult is not absolute, but is to take place "where appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation.

Chapter III – International co-operation

240. Chapter III contains a number of provisions relating to extradition and mutual legal assistance among the Parties.

Section 1 – General principles

Title 1 – General principles relating to international co-operation

General principles relating to international co-operation (Article 23)

241. Article 23 sets forth three general principles with respect to international co-operation under Chapter III.

242. Initially, the article makes clear that international co-operation is to be provided among Parties "to the widest extent possible." This principle requires Parties to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally.

243. Second, the general scope of the obligation to co-operate is set forth in Article 23: co-operation is to be extended to all criminal offences related to computer systems and data (i.e. the offences covered by Article 14, paragraph 2, *litterae a-b*), as well as to the collection of evidence in electronic form of a criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of Chapter III are applicable. However, it should be noted that Articles 24 (Extradition), 33 (Mutual assistance regarding the real time collection of traffic data) and 34 (Mutual assistance regarding the interception of content data) permit the Parties to provide for a different scope of application of these measures.

244. Finally, co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws." The latter clause establishes the general principle that the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements as between the parties thereto (described in greater detail in the discussion of Article 27 below), or relevant provisions of domestic law pertaining to international co-operation.

This basic principle is explicitly reinforced in Articles 24 (Extradition), 25 (General principles relating to mutual assistance), 26 (Spontaneous information), 27 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements), 28 (Confidentiality and limitation on use), 31 (Mutual assistance regarding accessing of stored computer data), 33 (Mutual assistance regarding the real-time collection of traffic data) and 34 (Mutual assistance regarding the interception of content data).

Title 2 – Principles relating to extradition

Extradition (Article 24)

245. Paragraph 1 specifies that the obligation to extradite applies only to offences established in accordance with Articles 2-11 of the Convention that 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. The drafters decided to insert a threshold penalty because, under the Convention, Parties may punish some of the offences with a relatively short maximum period of incarceration (e.g., Article 2 – illegal access – and Article 4 – data interference). Given this, the drafters did not believe it appropriate to require that each of the offences established in Articles 2-11 be considered *per se* extraditable. Accordingly, agreement was reached on a general requirement that an offence is to be considered extraditable if – as in Article 2 of the European Convention on Extradition (ETS N° 24) – the maximum punishment that could be imposed for the offence for which extradition was sought was at least one year's imprisonment. The determination of whether an offence is extraditable does not hinge on the actual penalty imposed in the particular case at hand, but instead on the maximum period that may legally be imposed for a violation of the offence for which extradition is sought.

246. At the same time, in accordance with the general principle that international co-operation under Chapter III should be carried out pursuant to instruments in force between the Parties, Paragraph 1 also provides that where a treaty on extradition or an arrangement on the basis of uniform or reciprocal legislation is in force between two or more Parties (see description of this term in discussion of Article 27 below) which provides for a different threshold for extradition, the threshold provided for in such treaty or arrangement shall apply. For example, many extradition treaties between European countries and non-European countries provide that an offence is extraditable only if the maximum punishment is greater than one year's imprisonment or there is a more severe penalty. In such cases, international extradition practitioners will

continue to apply the normal threshold under their treaty practice in order to determine whether an offence is extraditable. Even under the European Convention on Extradition (ETS N° 24), reservations may specify a different minimum penalty for extradition. Among Parties to that Convention, when extradition is sought from a Party that has entered such a reservation, the penalty provided for in the reservation shall be applied in determining whether the offence is extraditable.

247. Paragraph 2 provides that the offences described in paragraph 1 are to be deemed extraditable offences in any extradition treaty between or among the Parties, and are to be included in future treaties they may negotiate among themselves. This does not mean that extradition must be granted on every occasion on which a request is made but rather that the possibility of granting extradition of persons for such offences must be available. Under paragraph 5, Parties are able to provide for other requirements for extradition.

248. Under paragraph 3, a Party that would not grant extradition, either because it has no extradition treaty with the requesting Party or because the existing treaties would not cover a request made in respect of the offences established in accordance with this Convention, may use the Convention itself as a basis for surrendering the person requested, although it is not obligated to do so.

249. Where a Party, instead of relying on extradition treaties, utilises a general statutory scheme to carry out extradition, paragraph 4 requires it to include the offences described in Paragraph 1 among those for which extradition is available.

250. Paragraph 5 provides that the requested Party need not extradite if it is not satisfied that all of the terms and conditions provided for by the applicable treaty or law have been fulfilled. It is thus another example of the principle that co-operation shall be carried out pursuant to the terms of applicable international instruments in force between the Parties, reciprocal arrangements, or domestic law. For example, conditions and restrictions set forth in the European Convention on Extradition (ETS No. 24) and its Additional Protocols (ETS Nos. 86 and 98) will apply to Parties to those agreements, and extradition may be refused on such bases (e.g., Article 3 of the European Convention on Extradition provides that extradition shall be refused if the offence is considered political in nature, or if the request is considered to have been made for the purpose of prosecuting or punishing a person on account of, *inter alia,* race, religion, nationality or political opinion).

251. Paragraph 6 applies the principle "aut dedere aut judicare" (extradite or prosecute). Since many States refuse extradition of their nationals, offenders who are found in the Party of which they are a national may avoid responsibility for a crime committed in another Party unless local authorities are obliged to take action. Under paragraph 6, if another Party has sought extradition of the offender, and extradition has been refused on the grounds that the offender is a national of the requested Party, the requested Party must, upon request of the requesting Party, submit the case to its authorities for the purpose of prosecution. If the Party whose extradition request has been refused does not request submission of the case for local investigation and prosecution, there is no obligation on the requested Party to take action. Moreover, if no extradition request has been made, or if extradition has been denied on grounds other than nationality, this paragraph establishes no obligation on the requested Party to submit the case for domestic prosecution. In addition, paragraph 6 requires the local investigation and prosecution to be carried out with diligence; it must be treated as seriously "as in the case of any other offence of a comparable nature" in the Party submitting the case. That Party shall report the outcome of its investigation and proceedings to the Party that had made the request.

252. In order that each Party know to whom its requests for provisional arrest or extradition should be directed, paragraph 7 requires Parties to communicate to the Secretary General of the Council of Europe the name and address of its authorities responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. This provision has been limited to situations in which there is no extradition treaty in force between the Parties concerned because if a bilateral or multilateral extradition treaty is in force between the Parties (such as ETS N° 24), the Parties will know to whom extradition and provisional arrest requests are to be directed without the necessity of a registration requirement. The communication to the Secretary General must be made at the time of signature or when depositing the Party's instrument of ratification, acceptance, approval or accession. It should be noted that designation of an authority does not exclude the possibility of using the diplomatic channel.

Title 3 – General principles relating to mutual assistance

General principles relating to mutual assistance (Article 25)

253. The general principles governing the obligation to provide mutual assistance are set forth in paragraph 1. Co-operation is to be provided "to the

widest extent possible." Thus, as in Article 23 ("General principals relating to international co-operation"), mutual assistance is in principle to be extensive, and impediments thereto strictly limited. Second, as in Article 23, the obligation to co-operate applies in principle to both criminal offences related to computer systems and data (i.e. the offences covered by Article 14, paragraph 2, *litterae a-b,* and to the collection of evidence in electronic form of a criminal offence. It was agreed to impose an obligation to co-operate as to this broad class of crimes because there is the same need for streamlined mechanisms of international co-operation as to both of these categories. However, Articles 34 and 35 permit the Parties to provide for a different scope of application of these measures.

254. Other provisions of this Chapter will clarify that the obligation to provide mutual assistance is generally to be carried out pursuant to the terms of applicable mutual legal assistance treaties, laws and arrangements. Under paragraph 2, each Party is required to have a legal basis to carry out the specific forms of co-operation described in the remainder of the Chapter, if its treaties, laws and arrangements do not already contain such provisions. The availability of such mechanisms, particularly those in Articles 29 through 35 (Specific provisions – Titles 1, 2, 3), is vital for effective co-operation in computer related criminal matters.

255. Some Parties will not require any implementing legislation in order to apply the provisions referred to in paragraph 2, since provisions of international treaties that establish detailed mutual assistance regimes are considered to be self-executing in nature. It is expected that Parties will either be able to treat these provisions as self executing, already have sufficient flexibility under existing mutual assistance legislation to carry out the mutual assistance measures established under this Chapter, or will be able to rapidly enact any legislation required to do so.

256. Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted

and responded to. Paragraph 3 does so by (1) empowering the Parties to make urgent requests for co-operation through expedited means of communications, rather than through traditional, much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems; and (2) requiring the requested Party to use expedited means to respond to requests in such circumstances. Each Party is required to have the ability to apply this measure if its mutual assistance treaties, laws or arrangement do not already so provide. The listing of fax and e-mail is indicative in nature; any other expedited means of communication may be used as would be appropriate in the particular circumstances at hand. As technology advances, further expedited means of communicating will be developed that may be used to request mutual assistance. With respect to the authenticity and security requirement contained in the paragraph, the Parties may decide among themselves how to ensure the authenticity of the communications and whether there is a need for special security protections (including encryption) that may be necessary in a particularly sensitive case. Finally, the paragraph also permits the requested Party to require a formal confirmation sent through traditional channels to follow the expedited transmission, if it so chooses.

257. Paragraph 4 sets forth the principle that mutual assistance is subject to the terms of applicable mutual assistance treaties (MLATs) and domestic laws. These regimes provide safeguards for the rights of persons located in the requested Party that may become the subject of a request for mutual assistance. For example, an intrusive measure, such as search and seizure, is not executed on behalf of a requesting Party, unless the requested Party's fundamental requirements for such measure applicable in a domestic case have been satisfied. Parties also may ensure protection of rights of persons in relation to the items seized and provided through mutual legal assistance.

258. However, paragraph 4 does not apply if "otherwise specifically provided in this Chapter." This clause is designed to signal that the Convention contains several significant exceptions to the general principle. The first such exception has been seen in paragraph 2 of this article, which obliges each Party to provide for the forms of co-operation set forth in the remaining articles of the Chapter (such as preservation, real time collection of data, search and seizure, and maintenance of a 24/7 network), regardless of whether or not its MLATs, equivalent arrangements or mutual assistance laws currently provide for such measures. Another exception is found in Article 27 which is always to be applied to the execution of requests in lieu of the requested Party's domestic law governing international co-operation in the absence of an MLAT

or equivalent arrangement between the requesting and requested Parties. Article 27 provides a system of conditions and grounds for refusal. Another exception, specifically provided for in this paragraph, is that co-operation may not be denied, at least as far as the offences established in Articles 2 – 11 of the Convention are concerned, on the grounds that the requested Party considers the request to involve a "fiscal" offence. Finally, Article 29 is an exception in that it provides that preservation may not be denied on dual criminality grounds, although the possibility of a reservation is provided for in this respect.

259. Paragraph 5 is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance (for example, where a requested Party has reserved its right to require dual criminality with respect to the preservation of data under Article 29, paragraph 4 "Expedited preservation of stored computer data"), dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in denominating the offence. This provision was believed necessary in order to ensure that requested Parties do not adopt too rigid a test when applying dual criminality. Given differences in national legal systems, variations in terminology and categorisation of criminal conduct are bound to arise. If the conduct constitutes a criminal violation under both systems, such technical differences should not impede assistance. Rather, in matters in which the dual criminality standard is applicable, it should be applied in a flexible manner that will facilitate the granting of assistance.

Spontaneous information (Article 26)

260. This article is derived from provisions in earlier Council of Europe instruments, such as Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS N° 141) and Article 28 of the Criminal Law Convention on Corruption (ETS N° 173). More and more frequently, a Party possesses valuable information that it believes may assist another Party in a criminal investigation or proceeding, and which the Party conducting the investigation or proceeding is not aware exists. In such cases, no request for mutual assistance will be forthcoming. Paragraph 1 empowers the State in possession of the information to forward it to the other State without a prior request. The provision was thought useful because, under the laws of some States, such a positive grant of legal authority is needed in order

to provide assistance in the absence of a request. A Party is not obligated to spontaneously forward information to another Party; it may exercise its discretion in light of the circumstances of the case at hand. Moreover, the spontaneous disclosure of information does not preclude the disclosing Party, if it has jurisdiction, from investigating or instituting proceedings in relation to the facts disclosed.

261. Paragraph 2 addresses the fact that in some circumstances, a Party will only forward information spontaneously if sensitive information will be kept confidential or other conditions can be imposed on the use of information. In particular, confidentiality will be an important consideration in cases in which important interests of the providing State may be endangered should the information be made public, e.g., where there is a need to protect the identity of a means of collecting the information or the fact that a criminal group is being investigated. If advance inquiry reveals that the receiving Party cannot comply with a condition sought by the providing Party (for example, where it cannot comply with a condition of confidentiality because the information is needed as evidence at a public trial), the receiving Party shall advise the providing Party, which then has the option of not providing the information. If the receiving Party agrees to the condition, however, it must honour it. It is foreseen that conditions imposed under this article would be consistent with those that could be imposed by the providing Party pursuant to a request for mutual assistance from the receiving Party.

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

Procedures pertaining to mutual assistance requests in the absence of applicable international agreements (Article 27)

262. Article 27 obliges the Parties to apply certain mutual assistance procedures and conditions 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 article thus reinforces the general principle that mutual assistance should be carried out through application of relevant treaties and similar arrangements for mutual assistance. The drafters rejected the creation of a separate general regime of mutual assistance in this Convention that would be applied in lieu of other applicable instruments and arrangements, agreeing instead that it would be more practical to rely on existing MLAT regimes as a general matter, thereby permitting mutual assistance practitioners to use the instruments and arrangements they are the most

familiar with and avoiding confusion that may result from the establishment of competing regimes. As previously stated, only with respect to mechanisms particularly necessary for rapid effective co-operation in computer related criminal matters, such as those in Articles 29-35 (Specific provisions – Title 1, 2, 3), is each Party required to establish a legal basis to enable the carrying out of such forms of co-operation if its current mutual assistance treaties, arrangements or laws do not already do so.

263. Accordingly, most forms of mutual assistance under this Chapter will continue to be carried out pursuant to the European Convention on Mutual Assistance in Criminal Matters (ETS N° 30) and its Protocol (ETS N° 99) among the Parties to those instruments. Alternatively, Parties to this Convention that have bilateral MLATs in force between them, or other multilateral agreements governing mutual assistance in criminal cases (such as between member States of the European Union), shall continue to apply their terms, supplemented by the computer or computer-related crime-specific mechanisms described in the remainder of Chapter III, unless they agree to apply any or all of the provisions of this article in lieu thereof. Mutual assistance may also be based on arrangements agreed on the basis of uniform or reciprocal legislation, such as the system of co-operation developed among the Nordic countries, which is also admitted by the European Convention on Mutual Assistance in Criminal Matters (Article 25, paragraph 4), and among members of the Commonwealth. Finally, the reference to mutual assistance treaties or arrangements on the basis of uniform or reciprocal legislation is not limited to those instruments in force at the time of entry into force of the present Convention, but also covers instruments that may be adopted in the future.

264. Article 27 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements), paragraphs 2-10, provide a number of rules for providing mutual assistance in the absence of an MLAT or arrangement on the basis of uniform or reciprocal legislation, including establishment of central authorities, imposing of conditions, grounds for and procedures in cases of postponement or refusal, confidentiality of requests, and direct communications. With respect to such expressly covered issues, in the absence of a mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, the provisions of this article are to be applied in lieu of otherwise applicable domestic laws governing mutual assistance. At the same time, Article 27 does not provide rules for other issues typically dealt with in domestic legislation governing international mutual assistance. For example, there are no provisions dealing with the form and contents of requests, taking

of witness testimony in the requested or requesting Parties, the providing of official or business records, transfer of witnesses in custody, or assistance in confiscation matters. With respect to such issues, Article 25, paragraph 4 provides that absent a specific provision in this Chapter, the law of the requested Party shall govern specific modalities of providing that type of assistance.

265. Paragraph 2 requires the establishment of a central authority or authorities responsible for sending and answering requests for assistance. The institution of central authorities is a common feature of modern instruments dealing with mutual assistance in criminal matters, and it is particularly helpful in ensuring the kind of rapid reaction that is so useful in combating computer- or computer-related crime. Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly.

266. Parties are encouraged as a matter of efficiency to designate a single central authority for the purpose of mutual assistance; it would generally be most efficient for the authority designated for such purpose under a Party's MLATs, or domestic law to also serve as the central authority when this article is applicable. However, a Party has the flexibility to designate more than one central authority where this is appropriate under its system of mutual assistance. Where more than one central authority is established, the Party that has done so should ensure that each authority interprets the provisions of the Convention in the same way, and that both incoming and outgoing requests are treated rapidly and efficiently. Each Party is to advise the Secretary General of the Council of Europe of the names and addresses (including e-mail and fax numbers) of the authority or authorities designated to receive and respond to mutual assistance requests under this article, and Parties are obliged to ensure that the designation is kept up-to-date.

267. A major objective of a State requesting mutual assistance often is to ensure that its domestic laws governing the admissibility of evidence are fulfilled, and it can use the evidence before its courts as a result. To ensure that such evidentiary requirements can be met, paragraph 3 obliges the requested Party to execute requests in accordance with the procedures specified by the requesting Party, unless to do so would be incompatible with its law. It is emphasised that this paragraph relates only to the obligation to respect

technical procedural requirements, not to fundamental procedural protections. Thus, for example, a requesting Party cannot require the requested Party to execute a search and seizure that would not meet the requested Party's fundamental legal requirements for this measure. In light of the limited nature of the obligation, it was agreed that the mere fact that the requested Party's legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting Party; instead, the procedure must be incompatible with the requested Party's legal principles. For example, under the law of the requesting Party, it may be a procedural requirement that a statement of a witness be given under oath. Even if the requested Party does not domestically have the requirement that statements be given under oath, it should honour the requesting Party's request.

268. Paragraph 4 provides for the possibility of refusing requests for mutual assistance requests brought under this Article. Assistance may be refused on the grounds provided for in Article 25, paragraph 4 (i.e. grounds provided for in the law of the requested Party), including prejudice to the sovereignty of the State, security, *ordre public* or other essential interests, and where the offence is considered by the requested Party to be a political offence or an offence connected with a political offence. In order to promote the overriding principle of providing the widest measure of co-operation (see Articles 23, 25), grounds for refusal established by a requested Party should be narrow and exercised with restraint. They may not be so expansive as to create the potential for assistance to be categorically denied, or subjected to onerous conditions, with respect to broad categories of evidence or information.

269. In line with this approach, it was understood that apart from those grounds set out in Article 28, refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal. A broad, categorical, or systematic application of data protection principles to refuse cooperation is therefore precluded. Thus, the fact the Parties concerned have different systems of protecting the privacy of data (such as that the requesting Party does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting Party uses means other than the process of deletion to protect

the privacy or the accuracy of the personal data received by law enforcement authorities), do not as such constitute grounds for refusal. Before invoking "essential interests" as a basis for refusing co-operation, the requested Party should instead attempt to place conditions which would allow the transfer of the data. (see Article 27, paragraph 6 and paragraph 271 of this report).

270. Paragraphs 5 permits the requested Party to postpone, rather than refuse, assistance where immediate action on the request would be prejudicial to investigations or proceedings in the requested Party. For example, where the requesting Party has sought to obtain evidence or witness testimony for purposes of investigation or trial, and the same evidence or witness are needed for use at a trial that is about to commence in the requested Party, the requested Party would be justified in postponing the providing of assistance.

271. Paragraph 6 provides that where the assistance sought would otherwise be refused or postponed, the requested Party may instead provide assistance subject to conditions. If the conditions are not agreeable to the requesting Party, the requested Party may modify them, or it may exercise its right to refuse or postpone assistance. Since the requested Party has an obligation to provide the widest possible measure of assistance, it was agreed that both grounds for refusal and conditions should be exercised with restraint.

272. Paragraph 7 obliges the requested Party to keep the requesting Party informed of the outcome of the request, and requires reasons to be given in the case of refusal or postponement of assistance. The providing of reasons can, *inter alia,* assist the requesting Party to understand how the requested Party interprets the requirements of this article, provide a basis for consultation in order to improve the future efficiency of mutual assistance, and provide to the requesting Party previously unknown factual information about the availability or condition of witnesses or evidence.

273. There are times when a Party makes a request in a particularly sensitive case, or in a case in which there could be disastrous consequences if the facts underlying the request were to be made public prematurely. Paragraph 8 accordingly permits the requesting Party to request that the fact and content of the request be kept confidential. Confidentiality may not be sought, however, to the extent that it would undermine the requested Party's ability to obtain the evidence or information sought, e.g., where the information will need to be disclosed in order to obtain a court order needed to effect assistance, or where private persons possessing evidence will need to be made aware of the request in order for it to be successfully executed. If the requested Party

cannot comply with the request for confidentiality, it shall notify the requesting Party, which then has the option of withdrawing or modifying the request.

274. Central authorities designated in accordance with paragraph 2 shall communicate directly with one another. However, in case of urgency, requests for mutual legal assistance may be sent directly by judges and prosecutors of the requesting Party to the judges and prosecutors of the requested Party. The judge or prosecutor following this procedure must also address a copy of the request made to his own central authority with a view to its transmission to the central authority of the requested Party. Under *littera b,* requests may be channelled through Interpol. Authorities of the requested Party that receive a request falling outside their field of competence, are, pursuant to *littera c,* under a two-fold obligation. First, they must transfer the request to the competent authority of the requested Party. Second, they must inform the authorities of the requesting Party of the transfer made. Under *littera d,* requests may also be transmitted directly without the intervention of central authorities even if there is no urgency, as long as the authority of the requested Party is able to comply with the request without making use of coercive action. Finally, *littera e* enables a Party to inform the others, through the Secretary General of the Council of Europe, that, for reasons of efficiency, direct communications are to be addressed to the central authority.

Confidentiality and limitation on use (Article 28)

275. This provision specifically provides for limitations on use of information or material, in order to enable the requested Party, in cases in which such information or material is particularly sensitive, to ensure that its use is limited to that for which assistance is granted, or to ensure that it is not disseminated beyond law enforcement officials of the requesting Party. These restrictions provide safeguards that are available for, *inter alia,* data protection purposes.

276. As in the case of Article 27, Article 28 only applies 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. Where such treaty or arrangement is in force, its provisions on confidentiality and use limitations shall apply in lieu of the provisions of this article, unless the Parties thereto agree otherwise. This avoids overlap with existing bilateral and multilateral mutual legal assistance treaties (MLATs) and similar arrangements, thereby enabling practitioners to continue to operate under the normal well-understood regime rather than seeking to apply two competing, possibly contradictory, instruments.

277. Paragraph 2 allows the requested Party, when responding to a request for mutual assistance, to impose two types of conditions. First, it may request that the information or material furnished be kept confidential where the request could not be complied with in the absence of such condition, such as where the identity of a confidential informant is involved. It is not appropriate to require absolute confidentiality in cases in which the requested Party is obligated to provide the requested assistance, as this would, in many cases, thwart the ability of the requesting Party to successfully investigate or prosecute crime, e.g. by using the evidence in a public trial (including compulsory disclosure).

278. Second, the requested Party may make furnishing of the information or material dependent on the condition that it not be used for investigations or proceedings other than those stated in the request. In order for this condition to apply, it must be expressly invoked by the requested Party, otherwise, there is no such limitation on use by the requesting Party. In cases in which it is invoked, this condition will ensure that the information and material may only be used for the purposes foreseen in the request, thereby ruling out use of the material for other purposes without the consent of the requested Party. Two exceptions to the ability to limit use were recognised by the negotiators and are implicit in the terms of the paragraph. First, under fundamental legal principles of many States, if material furnished is evidence exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. In addition, most material furnished under mutual assistance regimes is intended for use at trial, normally a public proceeding (including compulsory disclosure). Once such disclosure takes place, the material has essentially passed into the public domain. In these situations, it is not possible to ensure confidentiality to the investigation or proceeding for which mutual assistance was sought.

279. Paragraph 3 provides that if the Party to which the information is forwarded cannot comply with the condition imposed, it shall notify the providing Party, which then has the option of not providing the information. If the receiving Party agrees to the condition, however, it must honour it.

280. Paragraph 4 provides that the requesting Party may be required to explain the use made of the information or material it has received under conditions described in paragraph 2, in order that the requested Party may ascertain whether such condition has been complied with. It was agreed that the requested Party may not call for an overly burdensome accounting e.g., of each time the material or information furnished was accessed.

Section 2 – Specific provisions

281. The aim of the present Section is to provide for specific mechanisms in order to take effective and concerted international action in cases involving computer-related offences and evidence in electronic form.

Title 1 – Mutual assistance regarding provisional measures

Expedited preservation of stored computer data (Article 29)

282. This article provides for a mechanism at the international level equivalent to that provided for in Article 16 for use at the domestic level. Paragraph 1 of this article authorises a Party to make a request for, and paragraph 3 requires each Party to have the legal ability to obtain, the expeditious preservation of data stored in the territory of the requested Party by means of a computer system, in order that the data not be altered, removed or deleted during the period of time required to prepare, transmit and execute a request for mutual assistance to obtain the data. Preservation is a limited, provisional measure intended to take place much more rapidly than the execution of a traditional mutual assistance. As has been previously discussed, computer data is highly volatile. With a few keystrokes, or by operation of automatic programs, it may be deleted, altered or moved, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. Thus, it was agreed that a mechanism was required in order to ensure the availability of such data pending the lengthier and more involved process of executing a formal mutual assistance request, which may take weeks or months.

283. While much more rapid than ordinary mutual assistance practice, this measure is at the same time less intrusive. The mutual assistance officials of the requested Party are not required to obtain possession of the data from its custodian. The preferred procedure is for the requested Party to ensure that the custodian (frequently a service provider or other third party) preserve (i.e., not delete) the data pending the issuance of process requiring it to be turned over to law enforcement officials at a later stage. This procedure has the advantage of being both rapid and protective of the privacy of the person whom the data concerns, as it will not be disclosed to or examined by any government official until the criteria for full disclosure pursuant to normal mutual assistance regimes have been fulfilled. At the same time, a requested Party is permitted to use other procedures for ensuring the rapid preservation of data, including the expedited issuance and execution of a production order

or search warrant for the data. The key requirement is to have an extremely rapid process in place to prevent the data from being irretrievably lost.

284. Paragraph 2 sets forth the contents of a request for preservation pursuant to this Article. Bearing in mind that this is a provisional measure and that a request will need to be prepared and transmitted rapidly, the information provided will be summary and include only the minimum information required to enable preservation of the data. In addition to specifying the authority that is seeking preservation and the offence for which the measure is sought, the request must provide a summary of the facts, information sufficient to identify the data to be preserved and its location, and a showing that the data is relevant to the investigation or prosecution of the offence concerned and that preservation is necessary. Finally, the requesting Party must undertake to subsequently submit a request for mutual assistance so that it may obtain production of the data.

285. Paragraph 3 sets forth the principle that dual criminality shall not be required as a condition to providing preservation. In general, application of the principle of dual criminality is counterproductive in the context of preservation. First, as a matter of modern mutual assistance practice, there is a trend to eliminate the dual criminality requirement for all but the most intrusive procedural measures, such as search and seizure or interception. Preservation as foreseen by the drafters, however, is not particularly intrusive, since the custodian merely maintains possession of data lawfully in its possession, and the data is not disclosed to or examined by officials of the requested Party until after execution of a formal mutual assistance request seeking disclosure of the data. Second, as a practical matter, it often takes so long to provide the clarifications necessary to conclusively establish the existence of dual criminality that the data would be deleted, removed or altered in the meantime. For example, at the early stages of an investigation, the requesting Party may be aware that there has been an intrusion into a computer in its territory, but may not until later have a good understanding of the nature and extent of damage. If the requested Party were to delay preserving traffic data that would trace the source of the intrusion pending conclusive establishment of dual criminality, the critical data would often be routinely deleted by service providers holding it for only hours or days after the transmission has been made. Even if thereafter the requesting Party were able to establish dual criminality, the crucial traffic data could not be recovered and the perpetrator of the crime would never be identified.

286. Accordingly, the general rule is that Parties must dispense with any dual criminality requirement for the purpose of preservation. However, a limited reservation is available under paragraph 4. If a Party requires dual criminality as a condition for responding to a request for mutual assistance for production of the data, and if it has reason to believe that, at the time of disclosure, dual criminality will not be satisfied, it may reserve the right to require dual criminality as a precondition to preservation. With respect to offences established in accordance with Articles 2 through 11, it is assumed that the condition of dual criminality is automatically met between the Parties, subject to any reservations they may have entered to these offences where permitted by the Convention. Therefore, Parties may impose this requirement only in relation to offences other than those defined in the Convention.

287. Otherwise, under paragraph 5, the requested Party may only refuse a request for preservation where its execution will prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. Due to the centrality of this measure to the effective investigation and prosecution of computer- or computer-related crime, it was agreed that the assertion of any other basis for refusing a request for preservation is precluded.

288. At times, the requested Party will realise that the custodian of the data is likely to take action that will threaten the confidentiality of, or otherwise prejudice, the requesting Party's investigation (for example, where the data to be preserved is held by a service provider controlled by a criminal group, or by the target of the investigation himself). In such situations, under paragraph 6, the requesting Party must be notified promptly, so that it may assess whether to take the risk posed by carrying through with the request for preservation, or to seek a more intrusive but safer form of mutual assistance, such as production or search and seizure.

289. Finally, paragraph 7 obliges each Party to ensure that data preserved pursuant to this Article will be held for at least 60 days pending receipt of a formal mutual assistance request seeking the disclosure of the data, and continue to be held following receipt of the request.

Expedited disclosure of preserved traffic data (Article 30)

290. This article provides the international equivalent of the power established for domestic use in Article 17. Frequently, at the request of a Party in which a crime was committed, a requested Party will preserve traffic data regarding

a transmission that has travelled through its computers, in order to trace the transmission to its source and identify the perpetrator of the crime, or locate critical evidence. In doing so, the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself. In such cases, the requested Party must expeditiously provide to the requesting Party a sufficient amount of the traffic data to enable identification of the service provider in, and path of the communication from, the other State. If the transmission came from a third State, this information will enable the requesting Party to make a request for preservation and expedited mutual assistance to that other State in order to trace the transmission to its ultimate source. If the transmission had looped back to the requesting Party, it will be able to obtain preservation and disclosure of further traffic data through domestic processes.

291. Under Paragraph 2, the requested Party may only refuse to disclose the traffic data, where disclosure is likely to prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. As in Article 29 (Expedited preservation of stored computer data), because this type of information is so crucial to identification of those who have committed crimes within the scope of this Convention or locating of critical evidence, grounds for refusal are to be strictly limited, and it was agreed that the assertion of any other basis for refusing assistance is precluded.

Title 2 – Mutual assistance regarding investigative powers

Mutual assistance regarding accessing of stored computer data (Article 31)

292. Each Party must have the ability to, for the benefit of another Party, search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within its territory – just as under Article 19 (Search and seizure of stored computer data) it must have the ability to do so for domestic purposes. Paragraph 1 authorises a Party to request this type of mutual assistance, and paragraph 2 requires the requested Party to be able to provide it. Paragraph 2 also follows the principle that the terms and conditions for providing such co-operation should be those set forth in applicable treaties, arrangements and domestic laws governing mutual legal assistance in criminal matters. Under paragraph 3, such a request must be responded to on an expedited basis where (1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or (2) otherwise where such treaties, arrangements or laws so provide.

Transborder access to stored computer data with consent or where publicly available (Article 32)

293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.

294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

Mutual assistance regarding the real-time collection of traffic data (Article 33)

295. In many cases, investigators cannot ensure that they are able to trace a communication to its source by following the trail through records of prior transmissions, as key traffic data may have been automatically deleted by a service provider in the chain of transmission before it could be preserved. It

is therefore critical for investigators in each Party to have the ability to obtain traffic data in real time regarding communications passing through a computer system in other Parties. Accordingly, under Article 33 (Mutual assistance regarding the real-time collection of traffic data), each Party is under the obligation to collect traffic data in real time for another Party. While this Article requires the Parties to co-operate on these matters, here, as elsewhere, deference is given to existing modalities of mutual assistance. Thus, the terms and conditions by which such co-operation is to be provided are generally those set forth in applicable treaties, arrangements and laws governing mutual legal assistance in criminal matters.

296. In many countries, mutual assistance is provided broadly with respect to the real time collection of traffic data, because such collection is viewed as being less intrusive than either interception of content data, or search and seizure. However, a number of States take a narrower approach. Accordingly, in the same way as the Parties may enter a reservation under Article 14 (Scope of procedural provisions), paragraph 3, with respect to the scope of the equivalent domestic measure, paragraph 2 permits Parties to limit the scope of application of this measure to a more narrow range of offences than provided for in Article 23 (General principles relating to international co-operation). One caveat is provided: in no event may the range of offences be more narrow than the range of offences for which such measure is available in an equivalent domestic case. Indeed, because real time collection of traffic data is at times the only way of ascertaining the identity of the perpetrator of a crime, and because of the lesser intrusiveness of the measure, the use of the term "at least" in paragraph 2 is designed to encourage Parties to permit as broad assistance as possible, i.e., even in the absence of dual criminality.

Mutual assistance regarding the interception of content data (Article 34)

297. Because of the high degree of intrusiveness of interception, the obligation to provide mutual assistance for interception of content data is restricted. The assistance is to be provided to the extent permitted by the Parties' applicable treaties and laws. As the provision of co-operation for interception of content is an emerging area of mutual assistance practice, it was decided to defer to existing mutual assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist. In this regard, reference is made to the comments on Articles 14, 15 and 21 as well as to N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications.

Title 3 – 24/7 Network

24/7 Network (Article 35)

298. As has been previously discussed, effective combating of crimes committed by use of computer systems and effective collection of evidence in electronic form requires very rapid response. Moreover, with a few keystrokes, action may be taken in one part of the world that instantly has consequences many thousands of kilometres and many time zones away. For this reason, existing police co-operation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively. The channel established in this Article is based upon the experience gained from an already functioning network created under the auspices of the G8 group of nations. Under this Article, each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings within the scope of this Chapter, in particular as defined under Article 35, paragraph 1, *litterae a – c*). It was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer or computer-related crime.

299. Each Party's 24/7 point of contact is to either facilitate or directly carry out, *inter alia,* the providing of technical advice, preservation of data, collection of evidence, giving of legal information, and locating of suspects. The term "legal information" in Paragraph 1 means advice to another Party that is seeking co-operation of any legal prerequisites required for providing informal or formal co-operation.

300. Each Party is at liberty to determine where to locate the point of contact within its law enforcement structure. Some Parties may wish to house the 24/7 contact within its central authority for mutual assistance, some may believe that the best location is with a police unit specialised in fighting computer or computer-related crime, yet other choices may be appropriate for a particular Party, given its governmental structure and legal system. Since the 24/7 contact is to provide both technical advice for stopping or tracing an attack, as well as such international co-operation duties as locating of suspects, there is no one correct answer, and it is anticipated that the structure of the network will evolve over time. In designating the national point of contact, due consideration should be given to the need to communicate with points of contacts using other languages.

301. Paragraph 2 provides that among the critical tasks to be carried out by the 24/7 contact is the ability to facilitate the rapid execution of those functions it does not carry out directly itself. For example, if a Party's 24/7 contact is part of a police unit, it must have the ability to co-ordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance, in order that appropriate action may be taken at any hour of the day or night. Moreover, paragraph 2 requires each Party's 24/7 contact to have the capacity to carry out communications with other members of the network on an expedited basis.

302. Paragraph 3 requires each point of contact in the network to have proper equipment. Up-to-date telephone, fax and computer equipment will be essential to the smooth operation of the network, and other forms of communication and analytical equipment will need to be part of the system as technology advances. Paragraph 3 also requires that personnel participating as part of a Party's team for the network be properly trained regarding computer- or computer-related crime and how to respond to it effectively.

Chapter IV – Final provisions

303. With some exceptions, the provisions contained in this Chapter are, for the most part, based on the "Model final clauses for conventions and agreements concluded within the Council of Europe' which were approved by the Committee of Ministers at the 315th meeting of the Deputies in February 1980. As most of the Articles 36 through 48 either use the standard language of the model clauses or are based on long-standing treaty-making practice at the Council of Europe, they do not call for specific comments. However, certain modifications of the standard model clauses or some new provisions require some explanation. It is noted in this context that the model clauses have been adopted as a non-binding set of provisions. As the Introduction to the Model Clauses pointed out "these model final clauses are only intended to facilitate the task of committees of experts and avoid textual divergences which would not have any real justification. The model is in no way binding and different clauses may be adapted to fit particular cases."

Signature and entry into force (Article 36)

304. Article 36, paragraph 1, has been drafted following several precedents established in other conventions elaborated within the framework of the Council of Europe, for instance, the Convention on the Transfer of Sentenced Persons (ETS No. 112) and the Convention on Laundering, Search, Seizure

and Confiscation of the Proceeds from Crime (ETS No. 141), which allow for signature, before their entry into force, not only by the member States of the Council of Europe, but also by non-member States which have participated in their elaboration. The provision is intended to enable the maximum number of interested States, not just members of the Council of Europe, to become Parties as soon as possible. Here, the provision is intended to apply to four non-member States, Canada, Japan, South Africa and the United States of America, which actively participated in the elaboration of the Convention. Once the Convention enters into force, in accordance with paragraph 3, other non-member States not covered by this provision may be invited to accede to the Convention in conformity with Article 37, paragraph 1.

305. Article 36, paragraph 3 sets the number of ratifications, acceptances or approvals required for the Convention's entry into force at 5. This figure is higher than the usual threshold (3) in Council of Europe treaties and reflects the belief that a slightly larger group of States is needed to successfully begin addressing the challenge of international computer or computer-related crime. The number is not so high, however, so as not to delay unnecessarily the Convention's entry into force. Among the five initial States, at least three must be Council of Europe members, but the two others could come from the four non-member States that participated in the Convention's elaboration. This provision would of course also allow for the Convention to enter into force based on expressions of consent to be bound by five Council of Europe member States.

Accession to the Convention (Article 37)

306. Article 37 has also been drafted on precedents established in other Council of Europe conventions, but with an additional express element. Under long-standing practice, the Committee of Ministers decides, on its own initiative or upon request, to invite a non-member State, which has not participated in the elaboration of a convention, to accede to the convention after having consulted all contracting Parties, whether member States or not. This implies that if any contracting Party objects to the non-member State's accession, the Committee of Ministers would usually not invite it to join the convention. However, under the usual formulation, the Committee of Ministers could – in theory – invite such a non-member State to accede to a convention even if a non-member State Party objected to its accession. This means that – in theory – no right of veto is usually granted to non-member States Parties in the process of extending Council of Europe treaties to other

non-member States. However, an express requirement that the Committee of Ministers consult with and obtain the unanimous consent of all Contracting States – not just members of the Council of Europe – before inviting a non-member State to accede to the Convention has been inserted. As indicated above, such a requirement is consistent with practice and recognises that all Contracting States to the Convention should be able to determine with which non-member States they are to enter into treaty relations. Nevertheless, the formal decision to invite a non-member State to accede will be taken, in accordance with usual practice, by the representatives of the contracting Parties entitled to sit on the Committee of Ministers. This decision requires the two-thirds majority provided for in Article 20.d of the Statute of the Council of Europe and the unanimous vote of the representatives of the contracting Parties entitled to sit on the Committee.

307. Federal States seeking to accede to the Convention, which intend to make a declaration under Article 41, are required to submit in advance a draft of the statement referred to in Article 41, paragraph 3, so that the Parties will be in a position to evaluate how the application of the federal clause would affect the prospective Party's implementation of the Convention (see paragraph 320).

Effects of the Convention (Article 39)

308. Article 39, paragraphs 1 and 2 address the Convention's relationship to other international agreements or arrangements. The subject of how conventions of the Council of Europe should relate to one another or to other treaties, bilateral or multilateral, concluded outside the Council of Europe is not dealt with by the Model Clauses referred to above. The usual approach utilised in Council of Europe conventions in the criminal law area (e.g., Agreement on Illicit Traffic by Sea (ETS N° 156)) is to provide that: (1) new conventions do not affect the rights and undertakings derived from existing international multilateral conventions concerning special matters; (2) Parties to a new convention may conclude bilateral or multilateral agreements with one another on the matters dealt with by the convention for the purposes of supplementing or strengthening its provisions or facilitating the application of the principles embodied in it; and (3) if two or more Parties to the new convention have already concluded an agreement or treaty in respect of a subject which is dealt with in the convention or otherwise have established their relations in respect of that subject, they shall be entitled to apply that agreement or treaty or to regulate those relations accordingly, in lieu of the new convention, provided this facilitates international co-operation.

309. Inasmuch as the Convention generally is intended to supplement and not supplant multilateral and bilateral agreements and arrangements between Parties, the drafters did not believe that a possibly limiting reference to "special matters" was particularly instructive and were concerned that it could lead to unnecessary confusion. Instead, paragraph 1 of Article 39 simply indicates that the present Convention supplements other applicable treaties or arrangements as between Parties and it mentions in particular three Council of Europe treaties as non-exhaustive examples: the 1957 European Convention on Extradition (ETS N° 24), the 1959 European Convention on Criminal Matters (ETS N° 30) and its 1978 Additional Protocol (ETS N° 99). Therefore, regarding general matters, such agreements or arrangements should in principle be applied by the Parties to the Convention on cybercrime. Regarding specific matters only dealt with by this Convention, the rule of interpretation *lex specialis derogat legi generali* provides that the Parties should give precedence to the rules contained in the Convention. An example is Article 30, which provides for the expedited disclosure of preserved traffic data when necessary to identify the path of a specified communication. In this specific area, the Convention, as *lex specialis,* should provide a rule of first resort over provisions in more general mutual assistance agreements.

310. Similarly, the drafters considered language making the application of existing or future agreements contingent on whether they "strengthen" or "facilitate" co-operation as possibly problematic, because, under the approach established in the international co-operation Chapter, the presumption is that Parties will apply relevant international agreements and arrangements.

311. Where there is an existing mutual assistance treaty or arrangement as a basis for co-operation, the present Convention would only supplement, where necessary, the existing rules. For example, this Convention would provide for the transmission of mutual assistance requests by expedited means of communications (see Article 25, paragraph 3) if such a possibility does not exist under the original treaty or arrangement.

312. Consistent with the Convention's supplementary nature and, in particular, its approach to international co-operation, paragraph 2 provides that Parties are also free to apply agreements that already are or that may in the future come into force. Precedent for such an articulation is found in the Transfer of Sentenced Persons Convention (ETS N° 112). Certainly, in the context of international co-operation, it is expected that application of other international agreements (many of which offer proven, longstanding formulas for international assistance) will in fact promote co-operation. Consistent

with the terms of the present Convention, Parties may also agree to apply its international co-operation provisions in lieu of such other agreements (see Article 27(1)). In such instances the relevant co-operation provisions set forth in Article 27 would supersede the relevant rules in such other agreements. As the present Convention generally provides for minimum obligations, Article 39, paragraph 2 recognises that Parties are free to assume obligations that are more specific in addition to those already set out in the Convention, when establishing their relations concerning matters dealt with therein. However, this is not an absolute right: Parties must respect the objectives and principles of the Convention when so doing and therefore cannot accept obligations that would defeat its purpose.

313. Further, in determining the Convention's relationship to other international agreements, the drafters also concurred that Parties may look for additional guidance to relevant provisions in the Vienna Convention on the Law of Treaties.

314. While the Convention provides a much-needed level of harmonisation, it does not purport to address all outstanding issues relating to computer or computer-related crime. Therefore, paragraph 3 was inserted to make plain that the Convention only affects what it addresses. Left unaffected are other rights, restrictions, obligations and responsibilities that may exist but that are not dealt with by the Convention. Precedent for such a "savings clause" may be found in other international agreements (e.g., UN Terrorist Financing Convention).

Declarations (Article 40)

315. Article 40 refers to certain articles, mostly in respect of the offences established by the Convention in the substantive law section, where Parties are permitted to include certain specified additional elements which modify the scope of the provisions. Such additional elements aim at accommodating certain conceptual or legal differences, which in a treaty of global ambition are more justified than they perhaps might be in a purely Council of Europe context. Declarations are considered acceptable interpretations of Convention provisions and should be distinguished from reservations, which permit a Party to exclude or to modify the legal effect of certain obligations set forth in the Convention. Since it is important for Parties to the Convention to know which, if any, additional elements have been attached by other Parties, there is an obligation to declare them to the Secretary General of the Council of Europe at the time of signature or when depositing an instrument of ratification,

acceptance, approval or accession. Such notification is particularly important concerning the definition of offences, as the condition of dual criminality will have to be met by the Parties when applying certain procedural powers. No numerical limit was felt necessary in respect of declarations.

Federal clause (Article 41)

316. Consistent with the goal of enabling the largest possible number of States to become Parties, Article 41 allows for a reservation which is intended to accommodate the difficulties federal States may face as a result of their characteristic distribution of power between central and regional authorities. Precedents exist outside the criminal law area for federal declarations or reservations to other international agreements.[11] Here, Article 41 recognises that minor variations in coverage may occur as a result of well-established domestic law and practice of a Party which is a federal State. Such variations must be based on its Constitution or other fundamental principles concerning the division of powers in criminal justice matters between the central government and the constituent States or territorial entities of a federal State. There was agreement among the drafters of the Convention that the operation of the federal clause would only lead to minor variations in the application of the Convention.

317. For example, in the United States, under its Constitution and fundamental principles of federalism, federal criminal legislation generally regulates conduct based on its effects on interstate or foreign commerce, while matters of minimal or purely local concern are traditionally regulated by the constituent States. This approach to federalism still provides for broad coverage of illegal conduct encompassed by this Convention under US federal criminal law, but recognises that the constituent States would continue to regulate conduct that has only minor impact or is purely local in character. In some instances, within that narrow category of conduct regulated by State but not federal law, a constituent State may not provide for a measure that would otherwise fall within the scope of this Convention. For example, an attack on a stand-alone personal computer, or network of computers linked together in a single building, may only be criminal if provided for under the law of the State in

11. E.g. Convention Relating to the Status of Refugees of 28 July 1951, Art. 34; Convention Relating to the Status of Stateless Persons of 28 September 1954, Art. 37; Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 10 June 1958, Art. 11; Convention for the Protection of World Cultural and Natural Heritage of 16 November 1972, Art. 34.

which the attack took place; however the attack would be a federal offence if access to the computer took place through the Internet, since the use of the Internet provides the effect on interstate or foreign commerce necessary to invoke federal law. The implementation of this Convention through United States federal law, or through the law of another federal State under similar circumstances, would be in conformity with the requirements of Article 41.

318. The scope of application of the federal clause has been restricted to the provisions of Chapter II (substantive criminal law, procedural law and jurisdiction). Federal States making use of this provision would still be under the obligation to co-operate with the other Parties under Chapter III, even where the constituent State or other similar territorial entity in which a fugitive or evidence is located does not criminalise conduct or does not have procedures required under the Convention.

319. In addition, paragraph 2 of Article 41 provides that a federal State, when making a reservation under paragraph 1 of this article, 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. In respect of provisions the implementation of which come within the legislative jurisdiction of the constituent States or other similar territorial entities, the federal government shall refer the provisions to the authorities of these entities with a favourable endorsement, encouraging them to take appropriate action to give them effect.

Reservations (Article 42)

320. Article 42 provides for a number of reservation possibilities. This approach stems from the fact that the Convention covers an area of criminal law and criminal procedural law which is relatively new to many States. In addition, the global nature of the Convention, which will be open to member and non-member States of the Council of Europe, makes having such reservation possibilities necessary. These reservation possibilities aim at enabling the largest number of States to become Parties to the Convention, while permitting such States to maintain certain approaches and concepts consistent with their domestic law. At the same time, the drafters endeavoured to restrict the possibilities for making reservations in order to secure to the largest possible extent the uniform application of the Convention by the Parties. Thus, no other reservations may be made than those enumerated. In addition,

reservations may only be made by a Party at the time of signature or upon deposit of its instrument of ratification, acceptance, approval or accession.

321. Recognising that for some Parties certain reservations were essential to avoid conflict with their constitutional or fundamental legal principles, Article 43 imposes no specific time limit for the withdrawal of reservations. Instead, they should be withdrawn as soon as circumstances so permit.

322. In order to maintain some pressure on the Parties and to make them at least consider withdrawing their reservations, the Convention authorises the Secretary General of the Council of Europe to periodically enquire about the prospects for withdrawal. This possibility of enquiry is current practice under several Council of Europe instruments. The Parties are thus given an opportunity to indicate whether they still need to maintain their reservations in respect of certain provisions and to withdraw, subsequently, those which no longer prove necessary. It is hoped that over time Parties will be able to remove as many of their reservations as possible so as promote the Convention's uniform implementation.

Amendments (Article 44)

323. Article 44 takes its precedent from the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS N° 141), where it was introduced as an innovation in respect of criminal law conventions elaborated within the framework of the Council of Europe. The amendment procedure is mostly thought to be for relatively minor changes of a procedural and technical character. The drafters considered that major changes to the Convention could be made in the form of additional protocols.

324. The Parties themselves can examine the need for amendments or protocols under the consultation procedure provided for in Article 46. The European Committee on Crime Problems (CDPC) will in this regard be kept periodically informed and required to take the necessary measures to assist the Parties in their efforts to amend or supplement the Convention.

325. In accordance with paragraph 5, any amendment adopted would come into force only when all Parties have informed the Secretary General of their acceptance. This requirement seeks to ensure that the Convention will evolve in a uniform manner.

Settlement of disputes (Article 45)

326. Article 45, paragraph 1, provides that the European Committee on Crime Problems (CDPC) should be kept informed about the interpretation and application of the provisions of the Convention. Paragraph 2 imposes an obligation on the Parties to seek a peaceful settlement of any dispute concerning the interpretation or the application of the Convention. Any procedure for solving disputes should be agreed upon by the Parties concerned. Three possible mechanisms for dispute-resolution are suggested by this provision: the European Committee on Crime Problems (CDPC) itself, an arbitral tribunal or the International Court of Justice.

Consultations of the Parties (Article 46)

327. Article 46 creates a framework for the Parties to consult regarding implementation of the Convention, the effect of significant legal, policy or technological developments pertaining to the subject of computer- or computer-related crime and the collection of evidence in electronic form, and the possibility of supplementing or amending the Convention. The consultations shall in particular examine issues that have arisen in the use and implementation of the Convention, including the effects of declarations and reservations made under Articles 40 and 42.

328. The procedure is flexible and it is left to the Parties to decide how and when to convene if they so wish. Such a procedure was believed necessary by the drafters of the Convention to ensure that all Parties to the Convention, including non-member States of the Council of Europe, could be involved – on an equal footing basis – in any follow-up mechanism, while preserving the competences of the European Committee on Crime Problems (CDPC). The latter shall not only be kept regularly informed of the consultations taking place among the Parties, but also facilitate those and take the necessary measures to assist the Parties in their efforts to supplement or amend the Convention. Given the needs of effective prevention and prosecution of cyber-crime and the associated privacy issues, the potential impact on business activities, and other relevant factors, the views of interested parties, including law enforcement, non-governmental and private sector organisations, may be useful to these consultations (see also paragraph 14).

329. Paragraph 3 provides for a review of the Convention's operation after 3 years of its entry into force, at which time appropriate amendments may be recommended. The CDPC shall conduct such review with the assistance of the Parties.

330. Paragraph 4 indicates that except where assumed by the Council of Europe it will be for the Parties themselves to finance any consultations carried out in accordance with paragraph 1 of Article 46. However, apart from the European Committee on Crime Problems (CDPC), the Council of Europe Secretariat shall assist the Parties in their efforts under the Convention.

First Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), Strasbourg, 28 January 2003

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as "the Convention"), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1. For the purposes of this Protocol:

"racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2. The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

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:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due

to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

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:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

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:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2. A Party may either:

a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts

constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2. A Party may either

a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

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, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Chapter III – Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol

1. Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, mutatis mutandis, to this Protocol.

2. The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

Chapter IV – Final provisions

Article 9 – Expression of consent to be bound

1. This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:

a. signature without reservation as to ratification, acceptance or approval; or

b. signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2. A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3. The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10 – Entry into force

1. This Protocol 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 have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.

2. In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

Article 11 – Accession

1. After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

2. Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

Article 12 – Reservations and declarations

1. Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession.

2. By a written notification addressed to the Secretary General of the Council of Europe, any Party 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 Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.

3. 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 in Article 5, paragraph 2.a, and Article 6, paragraph 2.a, of this Protocol.

Article 13 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. 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.

2. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

Article 14 – Territorial application

1. Any Party 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 Protocol shall apply.

2. Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Protocol to any other territory specified in the declaration. In respect of such territory, the Protocol 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.

3. Any 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 15 – Denunciation

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

2. Such 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 16 – 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 Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Protocol in accordance with its Articles 9, 10 and 11;

d. any other act, notification or communication relating to this Protocol.

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

Done at Strasbourg, this 28 January 2003, 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 Protocol, and to any State invited to accede to it.

Explanatory Report to the First Additional Protocol

The text of this Explanatory Report does not constitute an instrument providing an authoritative interpretation of the Protocol, although it might be of such a nature as to facilitate the application of the provisions contained therein. This Protocol will be opened for signature in Strasbourg, on 28 January 2003, on the occasion of the First Part of the 2003 Session of the Parliamentary Assembly.

Introduction

1. Since the adoption in 1948 of the Universal Declaration of Human Rights, the international community has made important progress in the fight against racism, racial discrimination, xenophobia and related intolerance. National and international laws have been enacted and a number of international human rights instruments have been adopted, in particular, the International Convention of New York of 1965 on the Elimination of All Forms of Racial Discrimination, concluded in the framework of the United Nations needs to be mentioned (CERD). Although progress has been made, yet, the desire for a world free of racial hatred and bias remains only partly fulfilled.

2. As technological, commercial and economic developments bring the peoples of the world closer together, racial discrimination, xenophobia and other forms of intolerance continue to exist in our societies. Globalisation carries risks that can lead to exclusion and increased inequality, very often along racial and ethnic lines.

3. In particular, the emergence of international communication networks like the Internet provide certain persons with modern and powerful means to support racism and xenophobia and enables them to disseminate easily and widely expressions containing such ideas. In order to investigate and prosecute such persons, international co-operation is vital. The Convention on Cybercrime (ETS No. 185) hereinafter referred to as "the Convention", was drafted to enable mutual assistance concerning computer related crimes in the broadest sense in a flexible and modern way. The purpose of this Protocol is twofold: firstly, harmonising substantive criminal law in the fight against racism and xenophobia on the Internet and, secondly, improving international co-operation in this area. This kind of harmonisation alleviates the fight against such crimes on the national and on the international level. Corresponding offences in domestic laws may prevent misuse of computer systems for a racist purpose by Parties whose laws in this area are less well defined. As a consequence, the exchange of useful common experiences in the practical

handling of cases may be enhanced too. International co-operation (especially extradition and mutual legal assistance) is facilitated, e.g. regarding requirements of double criminality.

4. The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention.

5. The Parliamentary Assembly, in its Opinion No. 226 (2001) concerning the Convention, recommended immediately drawing up a protocol to the Convention under the title "Broadening the scope of the convention to include new forms of offence", with the purpose of defining and criminalising, *inter alia,* the dissemination of racist propaganda.

6. The Committee of Ministers therefore entrusted the European Committee on Crime Problems (CDPC) and, in particular, its Committee of Experts on the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems (PC-RX), with the task of preparing a draft additional Protocol, a binding legal instrument open to the signature and ratification of Contracting Parties to the Convention, dealing in particular with the following:

i. the definition and scope of elements for the criminalisation of acts of a racist and xenophobic nature committed through computer networks, including the production, offering, dissemination or other forms of distribution of materials or messages with such content through computer networks;

ii. the extent of the application of substantive, procedural and international co-operation provisions in the Convention on Cybercrime to the investigation and prosecution of the offences to be defined under the additional Protocol.

7. This Protocol entails an extension of the Convention's scope, including its substantive, procedural and international co-operation provisions, so as to cover also offences of racist and xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour, the Protocol aims at improving the ability of the Parties to make use of the means and avenues of international cooperation set out in the Convention in this area.

Commentary on the articles of the Protocol

Chapter I – Common provisions

Article 1 – Purpose

8. The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

9. The provisions of the Protocol are of a mandatory character. To satisfy these obligations, States Parties have not only to enact appropriate legislation but also to ensure that it is effectively enforced.

Article 2 – Definition

Paragraph 1 – "Racist and xenophobic material"

10. Several legal instruments have been elaborated at an international and national level to combat racism or xenophobia. The drafters of this Protocol took account in particular of (i) the International Convention on the Elimination of All Forms of Racial Discrimination (CERD), (ii) Protocol No. 12 (ETS No. 177) to the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), (iii) the Joint Action of 15 July 1996 of the European Union adopted by the Council on the basis of Article K.3 of the Treaty on the European Union, concerning action to combat racism and xenophobia, (iv) the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance (Durban, 31 August- 8 September 2001), (v) the conclusions of the European Conference against racism (Strasbourg, 13 October 2000) (vi) the comprehensive study published by the European Commission against Racism and Intolerance (ECRI) published in August 2000 (CRI(2000)27) and (vii) the November 2001 Proposal by the European Commission for a Council Framework Decision on combating racism and xenophobia (in the framework of the European Union).

11. Article 10 of the ECHR recognises the right to freedom of expression, which includes the freedom to hold opinions and to receive and impart information and ideas. "Article 10 of the ECHR is applicable not only to information and ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any

sector of the population.[12] However, the European Court of Human Rights held that the State's actions to restrict the right to freedom of expression were properly justified under the restrictions of paragraph 2 of Article 10 of the ECHR, in particular when such ideas or expressions violated the rights of others. This Protocol, on the basis of national and international instruments, establishes the extent to which the dissemination of racist and xenophobic expressions and ideas violates the rights of others.

12. The definition contained in Article 2 refers to written material (e.g. texts, books, magazines, statements, messages, etc.), images (e.g. pictures, photos, drawings, etc.) or any other representation of thoughts or theories, of a racist and xenophobic nature, in such a format that it can be stored, processed and transmitted by means of a computer system.

13. The definition contained in Article 2 of this Protocol refers to certain conduct to which the content of the material may lead, rather than to the expression of feelings/belief/aversion as contained in the material concerned. The definition builds upon existing national and international (UN, EU) definitions and documents as far as possible.

14. The definition requires that such material advocates, promotes, incites hatred, discrimination or violence. "Advocates" refers to a plea in favour of hatred, discrimination or violence, "promotes" refers to an encouragement to or advancing hatred, discrimination or violence and "incites" refers to urging others to hatred, discrimination or violence.

15. The term "violence" refers to the unlawful use of force, while the term "hatred" refers to intense dislike or enmity.

16. When interpreting the term "discrimination", account should be taken of the ECHR (Article 14 and Protocol 12), and of the relevant case-law, as well as of Article 1 of the CERD. The prohibition of discrimination contained in the ECHR guarantees to everyone within the jurisdiction of a State Party equality in the enjoyment of the rights and freedoms protected by the ECHR itself. Article 14 of the ECHR provides for a general obligation for States, accessory to the rights and freedoms provided for by the ECHR. In this context, the term "discrimination" used in the Protocol refers to a different unjustified treatment given to persons or to a group of persons on the basis of certain characteristics. In the several judgments (such as the Belgian Linguistic case, the Abdulaziz, Cabales

12. See in this context, for instance, the Handyside judgment of 7 December 1976, Series A, No. 24, p. 23, para. 49.

and Balkandali judgment[13] the European Court of Human Rights stated that "a difference of treatment is discriminatory if it 'has no objective and reasonable justification', that is, if it does not pursue a 'legitimate aim' or if there is not a "reasonable relationship of proportionality between the means employed and the aim sought to be realised"'. Whether the treatment is discriminatory or not has to be considered in the light of the specific circumstances of the case. Guidance for interpreting the term "discrimination" can also be found in Article 1 of the CERD, where the term "racial discrimination" means "any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life".

17. Hatred, discrimination or violence, have to be directed against any individual or group of individuals, for the reason that they belong to a group distinguished by "race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors".

18. It should be noted that these grounds are not exactly the same as the grounds contained, for instance, in Article 1 of Protocol No. 12 to the ECHR, as some of those contained in the latter are alien to the concept of racism or xenophobia. The grounds contained in Article 2 of this Protocol are also not identical to those contained in the CERD, as the latter deals with "racial discrimination" in general and not "racism" as such. In general, these grounds are to be interpreted within their meaning in established national and international law and practice. However, some of them require further explanation as to their specific meaning in the context of this Protocol.

18. "Descent" refers mainly to persons or groups of persons who descend from persons who could be identified by certain characteristics (such as race or colour), but not necessarily all of these characteristics still exist. In spite of that, because of their descent, such persons or groups of persons may be subject to hatred, discrimination or violence. "Descent" does not refer to social origin.

20. The notion of "national origin" is to be understood in a broad factual sense. It may refer to individuals' histories, not only with regard to the nationality or origin of their ancestors but also to their own national belonging, irrespective

13. Abulaziz, Cabales and Balkandali, judgment of 28 May 1985, Series A No. 94, p. 32, para. 62; Belgian Linguistic case, judgment of 23 July 1968, Series A No. 6, p. 34, para. 10.

of whether from a legal point of view they still possess it. When persons possess more than one nationality or are stateless, the broad interpretation of this notion intends to protect them if they are discriminated on any of these grounds. Moreover, the notion of "national origin" may not only refer to the belonging to one of the countries that is internationally recognised as such, but also to minorities or other groups of persons, with similar characteristics.

21. The notion of "religion" often occurs in international instruments and national legislation. The term refers to conviction and beliefs. The inclusion of this term as such in the definition would carry the risk of going beyond the ambit of this Protocol. However, religion may be used as a pretext, an alibi or a substitute for other factors, enumerated in the definition. "Religion" should therefore be interpreted in this restricted sense.

Paragraph 2

22. By providing that the terms and expressions used in the Protocol shall be interpreted in the same manner as they are interpreted under the Convention, this Article ensures uniform interpretation of both. This means that the terms and expressions used in this Explanatory Report are to be interpreted in the same manner as such terms and expressions are interpreted in the Explanatory Report to the Convention.

Chapter II – Measures to be taken at national level

General considerations

23. The offences, as established in this Protocol, contain a number of common elements which were taken from the Convention. For the sake of clarity, the relating paragraphs of the Explanatory Report to the Convention are included hereafter.

24. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable *per se*, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability (e.g. for law enforcement purposes, for academic or research purposes). The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual

or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Protocol, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

25. All the offences contained in the Protocol must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. The drafters of the Protocol, as those of the Convention, agreed that the exact meaning of "intentionally" should be left to national interpretation. Persons cannot be held criminally liable for any of the offences in this Protocol, if they have not the required intent. It is not sufficient, for example, for a service provider to be held criminally liable under this provision, that such a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.

26. As regards the notion of "computer system", this is the same as contained in the Convention and explained in paragraphs 23 and 24 of its Explanatory Report. This constitutes an application of Article 2 of this Protocol (see also the explanation of Article 2 above).

Article 3 – Dissemination of racist and xenophobic material in a computer system

27. This article requires States Parties to criminalize distributing or otherwise making available racist and xenophobic material to the public through a computer system. The act of distributing or making available is only criminal if the intent is also directed to the racist and xenophobic character of the material.

28. "Distribution" refers to the active dissemination of racist and xenophobic material, as defined in Article 2 of the Protocol, to others, while "making available" refers to the placing on line of racist and xenophobic material for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such material.

29. The term "to the public" used in Article 3 makes it clear that private communications or expressions communicated or transmitted through a computer system fall outside the scope of this provision. Indeed, such communications or expressions, like traditional forms of correspondence, are protected by Article 8 of the ECHR.

30. Whether a communication of racist and xenophobic material is considered as a private communication or as a dissemination to the public, has to be determined on the basis of the circumstances of the case. Primarily, what counts is the intent of the sender that the message concerned will only be received by the pre-determined receiver. The presence of this subjective intent can be established on the basis of a number of objective factors, such as the content of the message, the technology used, applied security measures, and the context in which the message is sent. Where such messages are sent at the same time to more than one recipient, the number of the receivers and the nature of the relationship between the sender and the receiver/s is a factor to determine whether such a communication may be considered as private.

31. Exchanging racist and xenophobic material in chat rooms, posting similar messages in newsgroups or discussion fora, are examples of making such material available to the public. In these cases the material is accessible to any person. Even when access to the material would require authorisation by means of a password, the material is accessible to the public where such authorisation would be given to anyone or to any person who meets certain criteria. In order to determine whether the making available or distributing was to the public or not, the nature of the relationship between the persons concerned should be taken into account.

32. Paragraphs 2 and 3 are included to provide for a reservation possibility in very limited circumstances. They should be read in conjunction and in sequence. Therefore, a Party, firstly, has the possibility not to attach criminal liability to the conduct contained in this Article where the material advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. For instance, those remedies may be civil or administrative. Where a Party cannot, due to established principles of its legal system concerning freedom of expression, provide for such remedies, it may reserve the right not to implement the obligation under paragraph 1 of this article, provided that it concerns only the advocating, promoting or inciting to discrimination, which is not associated to hatred or violence. A Party may further restrict the scope of the reservation by requiring that the discrimination is, for instance, insulting, degrading, or threatening a group of persons.

Article 4 – Racist and xenophobic motivated threat

33. Most legislation provide for the criminalisation of threat in general. The drafters agreed to stress in the Protocol that, beyond any doubt, threats for racist and xenophobic motives are to be criminalized.

34. The notion of "threat" may refer to a menace which creates fear in the persons to whom the menace is directed, that they will suffer the commission of a serious criminal offence (e.g. affecting the life, personal security or integrity, serious damage to properties, etc., of the victim or their relatives). It is left to the States Parties to determine what is a serious criminal offence.

35. According to this article, the threat has to be addressed either to (i) a person for the reason that he or she belongs to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or to (ii) a group of persons which is distinguished by any of these characteristics. There is a no restriction that the threat should be public. This article also covers threats by private communications.

Article 5 – Racist and xenophobic motivated insult

36. Article 5 deals with the question of insulting publicly a person or a group of persons because they belong or are thought to belong to a group distinguished by specific characteristics. The notion of "insult" refers to any offensive, contemptuous or invective expression which prejudices the honour or the dignity of a person. It should be clear from the expression itself that the insult is directly connected with the insulted person's belonging to the group. Unlike in the case of threat, an insult expressed in private communications is not covered by this provision.

37. Paragraph 2(i) allows Parties to require that the conduct must also have the effect that the person or group of persons, not only potentially, but are also actually exposed to hatred, contempt or ridicule.

38. Paragraph 2(ii) allows Parties to enter reservations which go further, even to the effect that paragraph 1 does not apply to them.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

39. In recent years, various cases have been dealt with by national courts where persons (in public, in the media, etc.) have expressed ideas or theories which aim at denying, grossly minimising, approving or justifying the serious

crimes which occurred in particular during the second World War (in particular the Holocaust).The motivation for such behaviours is often presented with the pretext of scientific research, while they really aim at supporting and promoting the political motivation which gave rise to the Holocaust. Moreover, these behaviours have also inspired or, even, stimulated and encouraged, racist and xenophobic groups in their action, including through computer systems. The expression of such ideas insults (the memory of) those persons who have been victims of such evil, as well as their relatives. Finally, it threatens the dignity of the human community.

40. Article 6, which has a similar structure as Article 3, addresses this problem. The drafters agreed that it was important to criminalize expressions which deny, grossly minimise, approve or justify acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April 1945. This owing to the fact that the most important and established conducts, which had given rise to genocide and crimes against humanity, occurred during the period 1940-1945. However, the drafters recognised that, since then, other cases of genocide and crimes against humanity occurred, which were strongly motivated by theories and ideas of a racist and xenophobic nature. Therefore, the drafters considered it necessary not to limit the scope of this provision only to the crimes committed by the Nazi regime during the Second World War and established as such by the Nuremberg Tribunal, but also to genocides and crimes against humanity established by other international courts set up since 1945 by relevant international legal instruments (such as UN Security Council Resolutions, multilateral treaties, etc.). Such courts may be, for instance, the International Criminal Tribunals for the former Yugoslavia, for Rwanda, the Permanent International Criminal Court. This article allows to refer to final and binding decisions of future international courts, to the extent that the jurisdiction of such a court is recognised by the Party signatory to this Protocol.

41. The provision is intended to make it clear that facts of which the historical correctness has been established may not be denied, grossly minimised, approved or justified in order to support these detestable theories and ideas.

42. The European Court of Human Rights has made it clear that the denial or revision of "clearly established historical facts – such as the Holocaust – […] would be removed from the protection of Article 10 by Article 17" of the ECHR (see in this context the Lehideux and Isorni judgment of 23 September 1998).[14]

14. Lehideux and Isorni judgment of 23 September 1998, Reports 1998-VII, para. 47.

43. Paragraph 2 of Article 6 allows a Party either (i) to require, through a declaration, that the denial or the gross minimisation referred to in paragraph 1 of Article 6, is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or (ii) to make use of a reservation, by allowing a Party not to apply – in whole or in part – this provision.

Article 7 – Aiding and abetting

44. The purpose of this article is to establish as criminal offences aiding or abetting the commission of any of the offences under Articles 3-6. Contrary to the Convention, the Protocol does not contain the criminalisation of the attempt to commit the offences contained in it, as many of the criminalized conducts have a preparatory nature.

45. Liability arises for aiding or abetting where the person who commits a crime established in the Protocol is aided by another person who also intends that the crime be committed. For example, although the transmission of racist and xenophobic material through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section. Thus, there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision.

46. As with all the offences established in accordance with the Protocol, aiding or abetting must be committed intentionally.

Chapter III – Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol

47. Article 8 deals with the relationship between the Convention and this Protocol. This provision avoids the inclusion of a number of provisions of the Convention in this Protocol. It indicates that some of the provisions of the Convention apply, *mutatis mutandis*, to this Protocol (e.g. concerning ancillary liability and sanctions, jurisdictions and a part of the final provisions). Paragraph 2 reminds the Parties that the meaning as defined in the Convention should apply to the offences of the Protocol. For the sake of clarity, the relating articles are specified.

Chapter IV – Final provisions

48. The provisions contained in this Chapter are, for the most part, based on the "Model final clauses for conventions and agreements concluded within the Council of Europe" which were approved by the Committee of Ministers at the 315th meeting of the Deputies in February 1980. As most of the Articles 9 through 16 either use the standard language of the model clauses or are based on long-standing treaty-making practice at the Council of Europe, they do not call for specific comments. However, certain modifications of the standard model clauses or some new provisions require further explanation. It is noted in this context that the model clauses have been adopted as a non-binding set of provisions. As the introduction to the model clauses pointed out "these model final clauses are only intended to facilitate the task of committees of experts and avoid textual divergences which would not have any real justification. The model is in no way binding and different clauses may be adopted to fit particular cases" (see also in this context paragraphs 304-330 of the Explanatory Report to the Convention).

49. Paragraph 2 of Article 12 specifies that the Parties may make use of the reservation as defined in Articles 3, 5 and 6 of this Protocol. No other reservation may be made.

50. This Protocol is opened to signature only to the signatories to the Convention. The Protocol will enter into force three months after five Parties to the Convention have expressed their consent to be bound by it (Articles 9-10).

51. The Convention allows reservations concerning certain provisions which, through the connecting clause of Article 8 of the Protocol, may have an effect on the obligations of a Party under the Protocol as well. Nevertheless, a Party may notify the Secretary General that it will not apply this reservation in respect of the content of the Protocol. This is expressed in paragraph 2 of Article 12 of the Protocol.

52. However, where a Party did not make use of such reservation possibility under the Convention, it may have a need to restrict its obligations in relation with the offences of the Protocol. Paragraph 2 of Article 12 enables Parties to do so in relation to Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention.

Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence (ETS No. 224), Strasbourg, 12 May 2022

Preamble

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime (ETS No. 185, hereinafter "the Convention"), opened for signature in Budapest on 23 November 2001, signatories hereto,

Bearing in mind the reach and impact of the Convention in all regions of the world;

Recalling that the Convention is already supplemented by the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), opened for signature in Strasbourg on 28 January 2003 (hereinafter "the First Protocol"), as between Parties to that Protocol;

Taking into account existing Council of Europe treaties on co-operation in criminal matters as well as other agreements and arrangements on co-operation in criminal matters between Parties to the Convention;

Having regard also for the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by its amending Protocol (CETS No. 223), opened for signature in Strasbourg on 10 October 2018, and to which any State may be invited to accede;

Recognising the growing use of information and communication technology, including internet services, and increasing cybercrime, which is a threat to democracy and the rule of law and which many States also consider a threat to human rights;

Also recognising the growing number of victims of cybercrime and the importance of obtaining justice for those victims;

Recalling that governments have the responsibility to protect society and individuals against crime not only offline but also online, including through effective criminal investigations and prosecutions;

Aware that evidence of any criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions, and convinced that additional measures are needed to lawfully obtain such evidence in order to enable an effective criminal justice response and to uphold the rule of law;

Recognising the need for increased and more efficient co-operation between States and the private sector, and that in this context greater clarity or legal certainty is needed for service providers and other entities regarding the circumstances in which they may respond to direct requests from criminal justice authorities in other Parties for the disclosure of electronic data;

Aiming, therefore, to further enhance co-operation on cybercrime and the collection of evidence in electronic form of any criminal offence for the purpose of specific criminal investigations or proceedings through additional tools pertaining to more efficient mutual assistance and other forms of co-operation between competent authorities; co-operation in emergencies; and direct co-operation between competent authorities and service providers and other entities in possession or control of pertinent information;

Convinced that effective cross-border co-operation for criminal justice purposes, including between public and private sectors, benefits from effective conditions and safeguards for the protection of human rights and fundamental freedoms;

Recognising that the collection of electronic evidence for criminal investigations often concerns personal data, and recognising the requirement in many Parties to protect privacy and personal data in order to meet their constitutional and international obligations; and

Mindful of the need to ensure that effective criminal justice measures on cybercrime and the collection of evidence in electronic form are subject to conditions and safeguards, which shall provide for the adequate protection of human rights and fundamental freedoms, including rights arising pursuant to obligations that States have undertaken under applicable international human rights instruments, such as the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5) of the Council of Europe,

the 1966 United Nations International Covenant on Civil and Political Rights, the 1981 African Charter on Human and People's Rights, the 1969 American Convention on Human Rights and other international human rights treaties;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement:

a. the Convention as between the Parties to this Protocol; and

b. the First Protocol as between the Parties to this Protocol that are also Parties to the First Protocol.

Article 2 – Scope of application

1. Except as otherwise specified herein, the measures described in this Protocol shall be applied:

a. as between Parties to the Convention that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence; and

b. as between Parties to the First Protocol that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol.

2. Each Party shall adopt such legislative and other measures as may be necessary to carry out the obligations set forth in this Protocol.

Article 3 – Definitions

1. The definitions provided in Articles 1 and 18, paragraph 3, of the Convention apply to this Protocol.

2. For the purposes of this Protocol, the following additional definitions apply:

a. "central authority" means the authority or authorities designated under a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned, or, in the absence thereof, the authority or authorities designated by a Party under Article 27, paragraph 2.a, of the Convention;

b. "competent authority" means a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings;

c. "emergency" means a situation in which there is a significant and imminent risk to the life or safety of any natural person;

d. "personal data" means information relating to an identified or identifiable natural person;

e. "transferring Party" means the Party transmitting the data in response to a request or as part of a joint investigation team or, for the purposes of chapter II, section 2, a Party in whose territory a transmitting service provider or entity providing domain name registration services is located.

Article 4 – Language

1. Requests, orders and accompanying information submitted to a Party shall be in a language acceptable to the requested Party or the Party notified under Article 7, paragraph 5, or be accompanied by a translation into such a language.

2. Orders under Article 7 and requests under Article 6, and any accompanying information shall be:

a. submitted in a language of the other Party in which the service provider or entity accepts them under comparable domestic process;

b. submitted in another language acceptable to the service provider or entity; or

c. accompanied by a translation into one of the languages under paragraphs 2.a or 2.b.

Chapter II – Measures for enhanced co-operation

Section 1 – General principles applicable to Chapter II

Article 5 – General principles applicable to Chapter II

1. The Parties shall co-operate in accordance with the provisions of this chapter to the widest extent possible.

2. Section 2 of this chapter consists of Articles 6 and 7. It provides for procedures enhancing direct co-operation with providers and entities in the territory of another Party. Section 2 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned.

3. Section 3 of this chapter consists of Articles 8 and 9. It provides for procedures to enhance international co-operation between authorities for the disclosure of stored computer data. Section 3 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties.

4. Section 4 of this chapter consists of Article 10. It provides for procedures pertaining to emergency mutual assistance. Section 4 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties.

5. Section 5 of this chapter consists of Articles 11 and 12. Section 5 applies 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 section 5 shall not apply where such treaty or arrangement exists, except as provided in Article 12, paragraph 7. However, the Parties concerned may mutually determine to apply the provisions of section 5 in lieu thereof, if the treaty or arrangement does not prohibit it.

6. Where, in accordance with the provisions of this Protocol, the requested Party is permitted to make co-operation 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.

7. The provisions in this chapter do not restrict co-operation between Parties, or between Parties and service providers or other entities, through other applicable agreements, arrangements, practices, or domestic law.

Section 2 – Procedures enhancing direct co-operation with providers and entities in other Parties

Article 6 – Request for domain name registration information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of specific

criminal investigations or proceedings, to issue a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name.

2. Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law.

3. The request under paragraph 1 shall include:

a. the date on which the request was issued and the identity and contact details of the competent authority issuing the request;

b. the domain name about which information is sought and a detailed list of the information sought, including the particular data elements;

c. a statement that the request is issued pursuant to this Protocol, that the need for the information arises because of its relevance to a specific criminal investigation or proceeding and that the information will only be used for that specific criminal investigation or proceeding; and

d. the time frame within which and the manner in which to disclose the information and any other special procedural instructions.

4. If acceptable to the entity, a Party may submit a request under paragraph 1 in electronic form. Appropriate levels of security and authentication may be required.

5. In the event of non-co-operation by an entity described in paragraph 1, a requesting Party may request that the entity give a reason why it is not disclosing the information sought. The requesting Party may seek consultation with the Party in which the entity is located, with a view to determining available measures to obtain the information.

6. Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, or at any other time, communicate to the Secretary General of the Council of Europe the authority designated for the purpose of consultation under paragraph 5.

7. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 6. Each Party shall ensure that the details that it has provided for the register are correct at all times.

Article 7 – Disclosure of subscriber information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2.a. Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1.

b. At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, a Party may – with respect to orders issued to service providers in its territory – make the following declaration: "The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision".

3. The order under paragraph 1 shall specify:

a. the issuing authority and date issued;

b. a statement that the order is issued pursuant to this Protocol;

c. the name and address of the service provider(s) to be served;

d. the offence(s) that is/are the subject of the criminal investigation or proceeding;

e. the authority seeking the specific subscriber information, if not the issuing authority; and

f. a detailed description of the specific subscriber information sought.

4. The order under paragraph 1 shall be accompanied by the following supplemental information:

a. the domestic legal grounds that empower the authority to issue the order;

b. a reference to legal provisions and applicable penalties for the offence being investigated or prosecuted;

c. the contact information of the authority to which the service provider shall return the subscriber information, from which it can request further information, or to which it shall otherwise respond;

d. the time frame within which and the manner in which to return the subscriber information;

e. whether preservation of the data has already been sought, including the date of preservation and any applicable reference number;

f. any special procedural instructions;

g. if applicable, a statement that simultaneous notification has been made pursuant to paragraph 5; and

h. any other information that may assist in obtaining disclosure of the subscriber information.

5.a. A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, notify the Secretary General of the Council of Europe that, when an order is issued under paragraph 1 to a service provider in its territory, the Party requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding.

b. Whether or not a Party requires notification under paragraph 5.a, it may require the service provider to consult the Party's authorities in identified circumstances prior to disclosure.

c. The authorities notified under paragraph 5.a or consulted under paragraph 5.b may, without undue delay, instruct the service provider not to disclose the subscriber information if:

i. disclosure may prejudice criminal investigations or proceedings in that Party; or

ii. conditions or grounds for refusal would apply under Article 25, paragraph 4, and Article 27, paragraph 4, of the Convention had the subscriber information been sought through mutual assistance.

d. The authorities notified under paragraph 5.a or consulted under paragraph 5.b:

i. may request additional information from the authority referred to in paragraph 4.c for the purposes of applying paragraph 5.c and shall not disclose it to the service provider without that authority's consent; and

ii. shall promptly inform the authority referred to in paragraph 4.c if the service provider has been instructed not to disclose the subscriber information and give the reasons for doing so.

e. A Party shall designate a single authority to receive notification under paragraph 5.a and perform the actions described in paragraphs 5.b, 5.c and 5.d. The Party shall, at the time when notification to the Secretary General of the Council of Europe under paragraph 5.a is first given, communicate to the Secretary General the contact information of that authority.

f. The Secretary General of the Council of Europe shall set up and keep updated a register of the authorities designated by the Parties pursuant to paragraph 5.e and whether and under what circumstances they require notification pursuant to paragraph 5.a. Each Party shall ensure that the details that it provides for the register are correct at all times.

6. If acceptable to the service provider, a Party may submit an order under paragraph 1 and supplemental information under paragraph 4 in electronic form. A Party may provide notification and additional information under paragraph 5 in electronic form. Appropriate levels of security and authentication may be required.

7. If a service provider informs the authority in paragraph 4.c that it will not disclose the subscriber information sought, or if it does not disclose subscriber information in response to the order under paragraph 1 within thirty days of receipt of the order or the timeframe stipulated in paragraph 4.d, whichever time period is longer, the competent authorities of the issuing Party may then seek to enforce the order only via Article 8 or other forms of mutual assistance. Parties may request that a service provider give a reason for refusing to disclose the subscriber information sought by the order.

8. A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that an issuing Party shall seek disclosure of subscriber information from the service provider before seeking it under Article 8, unless the issuing Party provides a reasonable explanation for not having done so.

9. At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may:

a. reserve the right not to apply this article; or

b. if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this article to such numbers.

Section 3 – Procedures enhancing international co-operation between authorities for the disclosure of stored computer data

Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored

a. subscriber information, and

b. traffic data

in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings.

2. Each Party shall adopt such legislative and other measures as may be necessary to give effect to an order under paragraph 1 submitted by a requesting Party.

3. In its request, the requesting Party shall submit the order under paragraph 1, the supporting information and any special procedural instructions to the requested Party.

a. The order shall specify:

   i. the issuing authority and the date the order was issued;

   ii. a statement that the order is submitted pursuant to this Protocol;

   iii. the name and address of the service provider(s) to be served;

   iv the offence(s) that is/are the subject of the criminal investigation or proceeding;

   v the authority seeking the information or data, if not the issuing authority; and

   vi. a detailed description of the specific information or data sought.

b. The supporting information, provided for the purpose of assisting the requested Party to give effect to the order and which shall not be disclosed to the service provider without the consent of the requesting Party, shall specify:

i. the domestic legal grounds that empower the authority to issue the order;

ii. the legal provisions and applicable penalties for the offence(s) being investigated or prosecuted;

iii. the reason why the requesting Party believes that the service provider is in possession or control of the data;

iv a summary of the facts related to the investigation or proceeding;

v the relevance of the information or data to the investigation or proceeding;

vi. contact information of an authority or authorities that may provide further information;

vii. whether preservation of the information or data has already been sought, including the date of preservation and any applicable reference number; and

viii. whether the information has or data have already been sought by other means, and, if so, in what manner.

c. The requesting Party may request that the requested Party carry out special procedural instructions.

4. A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, that additional supporting information is required to give effect to orders under paragraph 1.

5. The requested Party shall accept requests in electronic form. It may require appropriate levels of security and authentication before accepting the request.

6.a. The requested Party, from the date of receipt of all the information specified in paragraphs 3 and 4, shall make reasonable efforts to serve the service provider within forty-five days, if not sooner, and shall order a return of requested information or data no later than:

i. twenty days for subscriber information; and

ii. forty-five days for traffic data.

b. The requested Party shall provide for the transmission of the produced information or data to the requesting Party without undue delay.

7. If the requested Party cannot comply with the instructions under paragraph 3.c in the manner requested, it shall promptly inform the requesting Party, and, if applicable, specify any conditions under which it could comply, following which the requesting Party shall determine whether the request should nevertheless be executed.

8. The requested Party may refuse to execute a request on the grounds established in Article 25, paragraph 4, or Article 27, paragraph 4, of the Convention or may impose conditions it considers necessary to permit execution of the request. The requested Party may postpone execution of requests for reasons established under Article 27, paragraph 5, of the Convention. The requested Party shall notify the requesting Party as soon as practicable of the refusal, conditions, or postponement. The requested Party shall also notify the requesting Party of other circumstances that are likely to delay execution of the request significantly. Article 28, paragraph 2.b, of the Convention shall apply to this article.

9. a. If the requesting Party cannot comply with a condition imposed by the requested Party under paragraph 8, it shall promptly inform the requested Party. The requested Party shall then determine if the information or material should nevertheless be provided.

b. If the requesting Party accepts the condition, it shall be bound by it. The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material.

10. Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe and keep up to date the contact information of the authorities designated:

a. to submit an order under this article; and

b. to receive an order under this article.

11. A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires that requests by other Parties under this article be submitted to it by the central authority of the requesting Party, or by such other authority as mutually determined between the Parties concerned.

12. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 10. Each Party shall ensure that the details that it has provided for the register are correct at all times.

13. At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may reserve the right not to apply this article to traffic data.

Article 9 – Expedited disclosure of stored computer data in an emergency

1.a. Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, for its point of contact for the 24/7 Network referenced in Article 35 of the Convention ("point of contact") to transmit a request to and receive a request from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data in that service provider's possession or control, without a request for mutual assistance.

b. A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it will not execute requests under paragraph 1.a seeking only the disclosure of subscriber information.

2. Each Party shall adopt such legislative and other measures as may be necessary to enable, pursuant to paragraph 1:

a. its authorities to seek data from a service provider in its territory following a request under paragraph 1;

b. a service provider in its territory to disclose the requested data to its authorities in response to a request under paragraph 2.a; and

c. its authorities to provide the requested data to the requesting Party.

3. The request under paragraph 1 shall specify:

a. the competent authority seeking the data and date on which the request was issued;

b. a statement that the request is issued pursuant to this Protocol;

c. the name and address of the service provider(s) in possession or control of the data sought;

d. the offence(s) that is/are the subject of the criminal investigation or proceeding and a reference to its legal provisions and applicable penalties;

e. sufficient facts to demonstrate that there is an emergency and how the data sought relate to it;

f. a detailed description of the data sought;

g. any special procedural instructions; and

h. any other information that may assist in obtaining disclosure of the requested data.

4. The requested Party shall accept a request in electronic form. A Party may also accept a request transmitted orally and may require confirmation in electronic form. It may require appropriate levels of security and authentication before accepting the request.

5. A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires requesting Parties, following the execution of the request, to submit the request and any supplemental information transmitted in support thereof, in a format and through such channel, which may include mutual assistance, as specified by the requested Party.

6. The requested Party shall inform the requesting Party of its determination on the request under paragraph 1 on a rapidly expedited basis and, if applicable, shall specify any conditions under which it would provide the data and any other forms of co-operation that may be available.

7.a. If a requesting Party cannot comply with a condition imposed by the requested Party under paragraph 6, it shall promptly inform the requested Party. The requested Party shall then determine whether the information or material should nevertheless be provided. If the requesting Party accepts the condition, it shall be bound by it.

b. The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material.

Section 4 –Procedures pertaining to emergency mutual assistance

Article 10 – Emergency mutual assistance

1. Each Party may seek mutual assistance on a rapidly expedited basis where it is of the view that an emergency exists. A request under this article shall include, in addition to the other contents required, a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it.

2. A requested Party shall accept such a request in electronic form. It may require appropriate levels of security and authentication before accepting the request.

3. The requested Party may seek, on a rapidly expedited basis, supplemental information in order to evaluate the request. The requesting Party shall provide such supplemental information on a rapidly expedited basis.

4. Once satisfied that an emergency exists and the other requirements for mutual assistance have been satisfied, the requested Party shall respond to the request on a rapidly expedited basis.

5. Each Party shall ensure that a person from its central authority or other authorities responsible for responding to mutual assistance requests is available on a twenty-four hour, seven-day-a-week basis for the purpose of responding to a request under this article.

6. The central authority or other authorities responsible for mutual assistance of the requesting and requested Parties may mutually determine that the results of the execution of a request under this article, or an advance copy thereof, may be provided to the requesting Party through a channel other than that used for the request.

7. 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, Article 27, paragraphs 2.b and 3 to 8, and Article 28, paragraphs 2 to 4, of the Convention shall apply to this article.

8. Where such a treaty or arrangement exists, this article shall be supplemented by the provisions of such treaty or arrangement unless the Parties concerned mutually determine to apply any or all of the provisions of the Convention referred to in paragraph 7 of this article, in lieu thereof.

9. Each Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that requests may also be sent directly to its judicial authorities, or through the channels of the International Criminal Police Organization (INTERPOL) or to its 24/7 point of contact established under Article 35 of the Convention. 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. Where a request is sent directly to a judicial authority of the requested Party and that authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform the requesting Party directly that it has done so.

Section 5 – Procedures pertaining to international co-operation in the absence of applicable international agreements

Article 11 – Video conferencing

1. A requesting Party may request, and the requested Party may permit, testimony and statements to be taken from a witness or expert by video conference. The requesting Party and the requested Party shall consult in order to facilitate resolution of any issues that may arise with regard to the execution of the request, including, as applicable: which Party shall preside; the authorities and persons that shall be present; whether one or both Parties shall administer particular oaths, warnings or give instructions to the witness or expert; the manner of questioning the witness or expert; the manner in which the rights of the witness or expert shall be duly ensured; the treatment of claims of privilege or immunity; the treatment of objections to questions or responses; and whether one or both Parties shall provide translation, interpretation and transcription services.

2.a. The central authorities of the requested and requesting Parties shall communicate directly with each other for the purposes of this article. A requested Party may accept a request in electronic form. It may require appropriate levels of security and authentication before accepting the request.

b. The requested Party shall inform the requesting Party of the reasons for not executing or for delaying the execution of the request. Article 27, paragraph 8, of the Convention applies to this article. Without prejudice to any other condition a requested Party may impose in accordance with this article, Article 28, paragraphs 2 to 4, of the Convention apply to this article.

3. A requested Party providing assistance under this article shall endeavour to obtain the presence of the person whose testimony or statement is sought. Where appropriate the requested Party may, to the extent possible under its law, take the necessary measures to compel a witness or expert to appear in the requested Party at a set time and location.

4. The procedures relating to the conduct of the video conference specified by the requesting Party shall be followed, except where incompatible with the domestic law of the requested Party. In case of incompatibility, or to the extent that the procedure has not been specified by the requesting Party, the requested Party shall apply the procedure under its domestic law unless otherwise mutually determined by the requesting and requested Parties.

5. Without prejudice to any jurisdiction under the domestic law of the requesting Party, where in the course of the video conference, the witness or expert:

a. makes an intentionally false statement when the requested Party has, in accordance with the domestic law of the requested Party, obliged such person to testify truthfully;

b. refuses to testify when the requested Party has, in accordance with the domestic law of the requested Party, obliged such person to testify; or

c. commits other misconduct that is prohibited by the domestic law of the requested Party in the course of such proceedings;

the person shall be sanctionable in the requested Party in the same manner as if such act had been committed in the course of its domestic proceedings.

6.a. Unless otherwise mutually determined between the requesting Party and the requested Party, the requested Party shall bear all costs related to the execution of a request under this article, except:

i. the fees of an expert witness;

ii. the costs of translation, interpretation and transcription; and

iii. costs of an extraordinary nature.

b. If the execution of a request would impose costs of an extraordinary nature, the requesting Party and the requested Party shall consult each other in order to determine the conditions under which the request may be executed.

7. Where mutually agreed upon by the requesting Party and the requested Party:

a. the provisions of this article may be applied for the purposes of carrying out audio conferences;

b. video conferencing technology may be used for purposes, or for hearings, other than those described in paragraph 1, including for the purposes of identifying persons or objects.

8. Where a requested Party chooses to permit the hearing of a suspect or accused person, it may require particular conditions and safeguards with respect to the taking of testimony or a statement from, or providing notifications or applying procedural measures to, such person.

Article 12 – Joint investigation teams and joint investigations

1. By mutual agreement, the competent authorities of two or more Parties may establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings, where enhanced coordination is deemed to be of particular utility. The competent authorities shall be determined by the respective Parties concerned.

2. The procedures and conditions governing the operation of joint investigation teams, such as their specific purposes; composition; functions; duration and any extension periods; location; organisation; terms of gathering, transmitting and using information or evidence; terms of confidentiality; and terms for the involvement of the participating authorities of a Party in investigative activities taking place in another Party's territory, shall be as agreed between those competent authorities.

3. A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval that its central authority must be a signatory to or otherwise concur in the agreement establishing the team.

4. Those competent and participating authorities shall communicate directly, except that Parties may mutually determine other appropriate channels of communication where exceptional circumstances require more central coordination.

5. Where investigative measures need to be taken in the territory of one of the Parties concerned, participating authorities from that Party may request

their own authorities to take those measures without the other Parties having to submit a request for mutual assistance. Those measures shall be carried out by that Party's authorities in its territory under the conditions that apply under domestic law in a national investigation.

6. Use of information or evidence provided by the participating authorities of one Party to participating authorities of other Parties concerned may be refused or restricted in the manner set forth in the agreement described in paragraphs 1 and 2. If that agreement does not set forth terms for refusing or restricting use, the Parties may use the information or evidence provided:

a. for the purposes for which the agreement has been entered into;

b. for detecting, investigating and prosecuting criminal offences other than those for which the agreement was entered into, subject to the prior consent of the authorities providing the information or evidence. However, consent shall not be required where fundamental legal principles of the Party using the information or evidence require that it disclose the information or evidence to protect the rights of an accused person in criminal proceedings. In that case, those authorities shall notify the authorities that provided the information or evidence without undue delay; or

c. to prevent an emergency. In that case, the participating authorities that received the information or evidence shall notify without undue delay the participating authorities that provided the information or evidence, unless mutually determined otherwise.

7. In the absence of an agreement described in paragraphs 1 and 2, joint investigations may be undertaken under mutually agreed terms on a case-by-case basis. This paragraph applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned.

Chapter III – Conditions and safeguards

Article 13 – Conditions and safeguards

In accordance with Article 15 of the Convention, each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties.

Article 14 – Protection of personal data

1. Scope

a. Except as otherwise provided in paragraphs 1.b and c, each Party shall process the personal data that it receives under this Protocol in accordance with paragraphs 2 to 15 of this article.

b. If, at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under this Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned.

c. If the transferring Party and the receiving Party are not mutually bound under an agreement described in paragraph 1.b, they may mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned in lieu of paragraphs 2 to 15.

d. Each Party shall consider that the processing of personal data pursuant to paragraphs 1.a and 1.b meets the requirements of its personal data protection legal framework for international transfers of personal data, and no further authorisation for transfer shall be required under that legal framework. A Party may only refuse or prevent data transfers to another Party under this Protocol for reasons of data protection under the conditions set out in paragraph 15 when paragraph 1.a applies; or under the terms of an agreement or arrangement referred to in paragraphs 1.b or c, when one of those paragraphs applies.

e. Nothing in this article shall prevent a Party from applying stronger safeguards to the processing by its own authorities of personal data received under this Protocol.

2. Purpose and use

a. The Party that has received personal data shall process them for the purposes described in Article 2. It shall not further process the personal data for an incompatible purpose, and it shall not further process the data when

this is not permitted under its domestic legal framework. This article shall not prejudice the ability of the transferring Party to impose additional conditions pursuant to this Protocol in a specific case, however, such conditions shall not include generic data protection conditions.

b. The receiving Party shall ensure under its domestic legal framework that personal data sought and processed are relevant to and not excessive in relation to the purposes of such processing.

3. Quality and integrity

Each Party shall take reasonable steps to ensure that personal data are maintained with such accuracy and completeness and are as up to date as is necessary and appropriate for the lawful processing of the personal data, having regard to the purposes for which they are processed.

4. Sensitive data

Processing by a Party of personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, or trade union membership; genetic data; biometric data considered sensitive in view of the risks involved; or personal data concerning health or sexual life; shall only take place under appropriate safeguards to guard against the risk of unwarranted prejudicial impact from the use of such data, in particular against unlawful discrimination.

5. Retention periods

Each Party shall retain the personal data only for as long as necessary and appropriate in view of the purposes of processing the data pursuant to paragraph 2. In order to meet this obligation, it shall provide in its domestic legal framework for specific retention periods or periodic review of the need for further retention of the data.

6. Automated decisions

Decisions producing a significant adverse effect concerning the relevant interests of the individual to whom the personal data relate may not be based solely on automated processing of personal data, unless authorised under domestic law and with appropriate safeguards that include the possibility to obtain human intervention.

7. Data security and security incidents

a. Each Party shall ensure that it has in place appropriate technological, physical and organisational measures for the protection of personal data, in

particular against loss or accidental or unauthorised access, disclosure, alteration or destruction ("security incident").

b. Upon discovery of a security incident in which there is a significant risk of physical or non-physical harm to individuals or to the other Party, the receiving Party shall promptly assess the likelihood and scale thereof and shall promptly take appropriate action to mitigate such harm. Such action shall include notification to the transferring authority or, for purposes of chapter II, section 2, the authority or authorities designated pursuant to paragraph 7.c. However, notification may include appropriate restrictions as to the further transmission of the notification; it may be delayed or omitted when such notification may endanger national security, or delayed when such notification may endanger measures to protect public safety. Such action shall also include notification to the individual concerned, unless the Party has taken appropriate measures so that there is no longer a significant risk. Notification to the individual may be delayed or omitted under the conditions set out in paragraph 12.a.i. The notified Party may request consultation and additional information concerning the incident and the response thereto.

c. Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to be notified under paragraph 7.b for the purposes of chapter II, section 2; the information provided may subsequently be modified.

8. Maintaining records

Each Party shall maintain records or have other appropriate means to demonstrate how an individual's personal data are accessed, used and disclosed in a specific case.

9. Onward sharing within a Party

a. When an authority of a Party provides personal data received initially under this Protocol to another authority of that Party, that other authority shall process it in accordance with this article, subject to paragraph 9.b.

b. Notwithstanding paragraph 9.a, a Party that has made a reservation under Article 17 may provide personal data it has received to its constituent States or similar territorial entities provided the Party has in place measures in order that the receiving authorities continue to effectively protect the data by providing for a level of protection of the data comparable to that afforded by this article.

c. In case of indications of improper implementation of this paragraph, the transferring Party may request consultation and relevant information about those indications.

10. Onward transfer to another State or international organisation

a. The receiving Party may transfer the personal data to another State or international organisation only with the prior authorisation of the transferring authority or, for purposes of chapter II, section 2, the authority or authorities designated pursuant to paragraph 10.b.

b. Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to provide authorisation for purposes of chapter II, section 2; the information provided may subsequently be modified.

11. Transparency and notice

a. Each Party shall provide notice through the publication of general notices, or through personal notice to the individual whose personal data have been collected, with regard to:

i. the legal basis for and the purpose(s) of processing;

ii. any retention or review periods pursuant to paragraph 5, as applicable;

iii. recipients or categories of recipients to whom such data are disclosed; and

iv access, rectification and redress available.

b. A Party may subject any personal notice requirement to reasonable restrictions under its domestic legal framework pursuant to the conditions set forth in paragraph 12.a.i.

c. Where the transferring Party's domestic legal framework requires giving personal notice to the individual whose data have been provided to another Party, the transferring Party shall take measures so that the other Party is informed at the time of transfer regarding this requirement and appropriate contact information. The personal notice shall not be given if the other Party has requested that the provision of the data be kept confidential, where the conditions for restrictions as set out in paragraph 12.a.i apply. Once these restrictions no longer apply and the personal notice can be provided, the other Party shall take measures so that the transferring Party is informed. If it has not yet been informed, the transferring Party is entitled to make requests to the

receiving Party which will inform the transferring Party whether to maintain the restriction.

12. Access and rectification

a. Each Party shall ensure that any individual, whose personal data have been received under this Protocol is entitled to seek and obtain, in accordance with processes established in its domestic legal framework and without undue delay:

i. a written or electronic copy of the documentation kept on that individual containing the individual's personal data and available information indicating the legal basis for and purposes of the processing, retention periods and recipients or categories of recipients of the data ("access"), as well as information regarding available options for redress; provided that access in a particular case may be subject to the application of proportionate restrictions permitted under its domestic legal framework, needed, at the time of adjudication, to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned;

ii. rectification when the individual's personal data are inaccurate or have been improperly processed; rectification shall include – as appropriate and reasonable considering the grounds for rectification and the particular context of processing – correction, supplementation, erasure or anonymisation, restriction of processing, or blocking.

b. If access or rectification is denied or restricted, the Party shall provide to the individual, in written form which may be provided electronically, without undue delay, a response informing that individual of the denial or restriction. It shall provide the grounds for such denial or restriction and provide information about available options for redress. Any expense incurred in obtaining access should be limited to what is reasonable and not excessive.

13. Judicial and non-judicial remedies

Each Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of this article.

14. Oversight

Each Party shall have in place one or more public authorities that exercise, alone or cumulatively, independent and effective oversight functions and

powers with respect to the measures set forth in this article. The functions and powers of these authorities acting alone or cumulatively shall include investigation powers, the power to act upon complaints and the ability to take corrective action.

15. Consultation and suspension

A Party may suspend the transfer of personal data to another Party if it has substantial evidence that the other Party is in systematic or material breach of the terms of this article or that a material breach is imminent. It shall not suspend transfers without reasonable notice, and not until after the Parties concerned have engaged in a reasonable period of consultation without reaching a resolution. However, a Party may provisionally suspend transfers in the event of a systematic or material breach that poses a significant and imminent risk to the life or safety of, or substantial reputational or monetary harm to, a natural person, in which case it shall notify and commence consultations with the other Party immediately thereafter. If the consultation has not led to a resolution, the other Party may reciprocally suspend transfers if it has substantial evidence that suspension by the suspending Party was contrary to the terms of this paragraph. The suspending Party shall lift the suspension as soon as the breach justifying the suspension has been remedied; any reciprocal suspension shall be lifted at that time. Any personal data transferred prior to suspension shall continue to be treated in accordance with this Protocol.

Chapter IV – Final provisions

Article 15 – Effects of this Protocol

1.a. Article 39, paragraph 2, of the Convention shall apply to this Protocol.

b. With respect to Parties that are members of the European Union, those Parties may, in their mutual relations, apply European Union law governing the matters dealt with in this Protocol.

c. Paragraph 1.b does not affect the full application of this Protocol between Parties that are members of the European Union and other Parties.

2. Article 39, paragraph 3, of the Convention shall apply to this Protocol.

Article 16 – Signature and entry into force

1. This Protocol shall be open for signature by Parties to the Convention, which may express their consent to be bound by either:

a. signature without reservation as to ratification, acceptance or approval; or

b. signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Protocol 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 Parties to the Convention have expressed their consent to be bound by this Protocol, in accordance with the provisions of paragraphs 1 and 2 of this article.

4. In respect of any Party to the Convention which subsequently expresses its consent to be bound by this Protocol, this Protocol 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 the Party has expressed its consent to be bound by this Protocol, in accordance with the provisions of paragraphs 1 and 2 of this article.

Article 17 – Federal clause

1. A federal State may reserve the right to assume obligations under this Protocol consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities, provided that:

a. this Protocol shall apply to the central government of the federal State;

b. such a reservation shall not affect obligations to provide for the co-operation sought by other Parties in accordance with the provisions of Chapter II; and

c. the provisions of Article 13 shall apply to the federal State's constituent States or other similar territorial entities.

2. Another Party may prevent authorities, providers or entities in its territory from co-operating in response to a request or order submitted directly by the constituent State or other similar territorial entity of a federal State that has made a reservation under paragraph 1, unless that federal State notifies the Secretary General of the Council of Europe that a constituent State or other similar territorial entity applies the obligations of this Protocol applicable to

that federal State. The Secretary General of the Council of Europe shall set up and keep updated a register of such notifications.

3. Another Party shall not prevent authorities, providers, or entities in its territory from co-operating with a constituent State or other similar territorial entity on the grounds of a reservation under paragraph 1, if an order or request has been submitted via the central government or a joint investigation team agreement under Article 12 is entered into with the participation of the central government. In such situations, the central government shall provide for the fulfilment of the applicable obligations of this Protocol, provided that, with respect to the protection of personal data provided to constituent States or similar territorial entities, only the terms of Article 14, paragraph 9, or, where applicable, the terms of an agreement or arrangement described in Article 14, paragraphs 1.b or 1.c, shall apply.

4. With regard to the provisions of this Protocol, 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 central 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 18 – Territorial application

1. This Protocol shall apply to the territory or territories specified in a declaration made by a Party under Article 38, paragraphs 1 or 2, of the Convention to the extent that such declaration has not been withdrawn under Article 38, paragraph 3.

2. A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that this Protocol shall not apply to one or more territories specified in the Party's declaration under Article 38, paragraphs 1 and/or 2, of the Convention.

3. A declaration under paragraph 2 of this article 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 19 – Reservations and declarations

1. By a written notification addressed to the Secretary General of the Council of Europe, any Party to the Convention may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it avails itself of the reservation(s) provided for in Article 7, paragraphs 9.a and 9.b, Article 8, paragraph 13, and Article 17 of this Protocol. No other reservations may be made.

2. By a written notification addressed to the Secretary General of the Council of Europe, any Party to the Convention may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, make the declaration(s) identified in Article 7, paragraphs 2.b and 8; Article 8, paragraph 11; Article 9, paragraphs 1.b and 5; Article 10, paragraph 9; Article 12, paragraph 3; and Article 18, paragraph 2, of this Protocol.

3. By a written notification addressed to the Secretary General of the Council of Europe, any Party to the Convention shall make any declaration(s), notifications or communications identified in Article 7, paragraphs 5.a and 5.e; Article 8, paragraphs 4, 10.a and 10.b; Article 14, paragraphs 7.c and 10.b; and Article 17, paragraph 2, of this Protocol according to the terms specified therein.

Article 20 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 19, paragraph 1, shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. 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 this later date.

2. The Secretary General of the Council of Europe may periodically enquire of Parties that have made one or more reservations in accordance with Article 19, paragraph 1, as to the prospects for withdrawing such reservation(s).

Article 21 – Amendments

1. Amendments to this Protocol may be proposed by any Party to this Protocol and shall be communicated by the Secretary General of the Council

of Europe, to the member States of the Council of Europe and to the Parties and signatories to the Convention as well as to any State which has been invited to accede to the Convention.

2. Any 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.

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

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

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

Article 22 – Settlement of disputes

Article 45 of the Convention shall apply to this Protocol.

Article 23 – Consultations of the Parties and assessment of implementation

1. Article 46 of the Convention shall apply to this Protocol.

2. Parties shall periodically assess the effective use and implementation of the provisions of this Protocol. Article 2 of the Cybercrime Convention Committee Rules of Procedure as revised on 16 October 2020 shall apply mutatis mutandis. The Parties shall initially review and may modify by consensus the procedures of that article as they apply to this Protocol five years after the entry into force of this Protocol.

3. The review of Article 14 shall commence once ten Parties to the Convention have expressed their consent to be bound by this Protocol.

Article 24 – Denunciation

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

2. Such 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.

3. Denunciation of the Convention by a Party to this Protocol constitutes denunciation of this Protocol.

4. Information or evidence transferred prior to the effective date of denunciation shall continue to be treated in accordance with this Protocol.

Article 25 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the Parties and signatories to the Convention, and any State which has been invited to accede to the Convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance or approval;

c. any date of entry into force of this Protocol in accordance with Article 16, paragraphs 3 and 4;

d. any declarations or reservations made in accordance with Article 19 or withdrawal of reservations made in accordance with Article 20;

e. any other act, notification or communication relating to this Protocol.

Explanatory Report to the Second Additional Protocol

1. The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence ("this Protocol") was adopted by the Committee of Ministers of the Council of Europe at its 1417bis meeting (17 November 2021) of the Ministers' Deputies and this Protocol will be opened for signature in Strasbourg on 12 May 2022. The Committee of Ministers also took note of the explanatory report.

2. The text of this explanatory report is intended to guide and assist Parties in the application of this Protocol and reflects the understanding of the drafters as to its operation.

Introduction

Background

3. The Convention on Cybercrime (ETS No. 185, hereinafter "the Convention"), since its opening for signature in Budapest on 23 November 2001, has become an instrument with membership from and impact in all regions of the world.

4. In 2003, the Convention was supplemented by the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189, hereinafter "the First Protocol").

5. Information and communication technology has evolved and transformed societies globally in an extraordinary manner since the Convention was opened for signature in 2001. However, since then, there has also been a significant increase in the exploitation of technology for criminal purposes. Cybercrime is now considered by many Parties a serious threat to human rights, the rule of law and to the functioning of democratic societies. The threats posed by cybercrime are numerous. Examples include online sexual violence against children and other offences against the dignity and integrity of individuals; the theft and misuse of personal data that affect the private life of individuals; election interference and other attacks against democratic institutions; attacks against critical infrastructure, such as distributed denial of service and ransomware attacks; or the misuse of such technology for terrorist purposes. In 2020 and 2021, during the Covid-19 pandemic, countries observed significant Covid-19 related cybercrime, including attacks on hospitals and medical facilities developing vaccines against the virus; misuse of domain names to promote fake vaccines, treatments and cures; and other types of fraudulent activity.

6. Despite the growth of data-driven technologies and the pernicious expansion and evolution of cybercrime, the concepts embodied in the Convention are technology-neutral so that the substantive criminal law may be applied to both current and future technologies involved, and the Convention remains crucial in the fight against cybercrime. The Convention is aimed principally at (i) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime; (ii) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences, as well as of other offences committed by means of a computer system or relating to the use of electronic evidence of other crimes; and (iii) setting up a fast and effective regime of international co-operation.

7. In applying the Convention, the Parties respect the responsibility that governments have to protect individuals against crime, whether it is committed on- or offline, through effective criminal investigations and prosecutions. Indeed, some Parties to the Convention consider that they are bound by an international obligation to provide the means for the protection against crimes committed by means of a computer system (see *K.U. v. Finland*, European Court of Human Rights (Application No. 2872/02, judgment/decision of 2 March 2009), referencing the procedures and powers for criminal investigations or proceedings that the Parties must establish pursuant to the Convention).

8. The Parties have continually sought to fulfil their commitment to counter cybercrime by relying on various mechanisms and bodies created under the Convention and by taking the necessary steps to enable more effective criminal investigations and proceedings. Significantly, the use and implementation of the Convention are facilitated by the Cybercrime Convention Committee (T-CY) established under Article 46 of the Convention. Moreover, the Convention is supported by capacity-building programmes implemented by the Council of Europe's Cybercrime Programme Office in Bucharest, Romania, which assist countries worldwide in the implementation of the Convention. This triad of (i) the common standards of the Convention in the area of cybercrime, coupled with (ii) a robust mechanism for ongoing Party engagement through the T-CY and (iii) emphasis on capacity-building programmes has contributed significantly to the reach and impact of the Convention.

9. In 2012, the T-CY, in line with its mandate under Article 46, paragraph 1, of the Convention, to exchange "information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form" and to consider "possible supplementation or amendment of the Convention", set up the Ad hoc Subgroup on Jurisdiction

and Transborder Access to Data ("Transborder Group"). In December 2014, the T-CY also completed an assessment of the mutual assistance provisions of the Convention on Cybercrime and adopted a set of recommendations, including some that were to be addressed in a new protocol to the Convention. These efforts led to the creation in 2015 of the Working Group on Criminal Justice Access to Evidence Stored in the Cloud, including through Mutual Legal Assistance ("Cloud Evidence Group").

10. In 2016, the Cloud Evidence Group concluded, among other things, that "cybercrime, the number of devices, services and users (including of mobile devices and services) and with these the number of victims have reached proportions so that only a minuscule share of cybercrime or other offences involving electronic evidence will ever be recorded and investigated. The vast majority of victims of cybercrime cannot expect that justice will be served". The main challenges identified by the group were related to "cloud computing, territoriality and jurisdiction" and thus to the difficulties of obtaining efficient access to or the disclosure of electronic evidence.

11. In reviewing the conclusions of the Cloud Evidence Group, the Parties to the Convention concluded that there was no need to amend the Convention or to provide for additional criminalisation through substantive criminal law provisions. The Parties determined, however, that additional measures were needed to enhance co-operation and the ability of criminal justice authorities to obtain electronic evidence through a second additional protocol in order to enable a more effective criminal justice response and to uphold the rule of law.

The preparatory work

12. The 17th plenary session of the T-CY (8 June 2017) approved the terms of reference for the preparation of this Protocol based on a proposal prepared by the T-CY Cloud Evidence Group. It decided to start the drafting of this Protocol at its own initiative under Article 46, paragraph 1.c, of the Convention. On 14 June 2017, the Deputy Secretary General of the Council of Europe informed the Committee of Ministers (1289th meeting of the Ministers' Deputies) of this T-CY initiative.

13. The terms of reference initially covered the period from September 2017 to December 2019 and they were subsequently extended by the T-CY to December 2020 and again to May 2021.

14. Under these terms of reference, the T-CY set up a Protocol Drafting Plenary (PDP) consisting of representatives of Parties to the Convention, and of States, organisations and Council of Europe bodies with observer status in the T-CY, as observers. The PDP was assisted in the preparation of the draft protocol by a Protocol Drafting Group (PDG) consisting of experts from Parties to the Convention. The PDG in turn set up several subgroups and ad hoc groups to work on specific provisions.

15. Between September 2017 and May 2021, the T-CY held 10 drafting plenaries, 16 drafting group meetings and numerous sub- and ad hoc group meetings. Much of this Protocol was prepared during the Covid-19 pandemic. Because of Covid-19 related restrictions, between March 2020 and May 2021, more than 65 meetings were held in virtual format.

16. The above working methods in plenaries, drafting groups and sub- and ad hoc groups permitted representatives and experts from Parties to contribute extensively to the drafting of this Protocol and to develop innovative solutions.

17. The Commission of the European Union participated in this work on behalf of the States Parties to the Convention that were members of the European Union under a negotiation mandate given by the Council of the European Union on 6 June 2019.

18. Once draft provisions had been prepared and provisionally adopted by the PDP, the draft articles were published and stakeholders were invited to provide comments.

19. The T-CY held six rounds of consultations with stakeholders from civil society and the private sector, and with data protection experts. This was in conjunction with the Octopus Conference on co-operation against cybercrime in Strasbourg in July 2018; with data protection experts in Strasbourg in November 2018; via invitation for written comments on draft articles in February 2019; in conjunction with the Octopus Conference on co-operation against cybercrime in Strasbourg in November 2019; via invitation for written comments on further draft articles in December 2020; and in May 2021 via written submissions and a virtual meeting held on 6 May 2021.

20. The T-CY furthermore consulted the European Committee on Crime Problems (CDPC) and the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe.

21. The 24th plenary of the T-CY on 28 May 2021 approved the draft of this Protocol and decided to submit it to the Committee of Ministers in view of adoption.

Substantive considerations

22. In terms of substance, the starting point for the work on this Protocol was the results of the T-CY assessment of the mutual assistance provisions of the Convention in 2014 and the analyses and recommendations of the T-CY Transborder Group and Cloud Evidence Group in 2014 and 2017 respectively. Of particular concern were the challenges of territoriality and jurisdiction related to electronic evidence, that is, that specified data needed in a criminal investigation may be stored in multiple, shifting or unknown jurisdictions ("in the cloud"), and that solutions are needed to obtain the disclosure of such data in an effective and efficient manner for the purpose of specific criminal investigations or proceedings.

23. Given the complexity of these challenges, the drafters of this Protocol agreed to focus on the following specific issues:

- At the time of drafting this Protocol, mutual assistance requests were the primary method to obtain electronic evidence of a criminal offence from other States, including the mutual assistance tools of the Convention. However, mutual assistance is not always an efficient way to process an increasing number of requests for volatile electronic evidence. Therefore, it was considered necessary to develop a more streamlined mechanism for issuing orders or requests to service providers in other Parties to produce subscriber information and traffic data.
- Subscriber information – for example, to identify the user of a specific e-mail or social media account or of a specific Internet Protocol (IP) address used in the commission of an offence – is the most often sought information in domestic and international criminal investigations relating to cybercrime and other crimes involving electronic evidence. Without this information, it is often impossible to proceed with an investigation. Obtaining subscriber information through mutual assistance in most cases is not effective and overburdens the mutual assistance system. Subscriber information is normally held by service providers. While Article 18 of the Convention already addresses some aspects of obtaining subscriber information from service providers (see the T-CY Guidance Note on Article 18), including in other Parties, complementary tools were found to be necessary to obtain the disclosure of subscriber information

directly from a service provider in another Party. These tools would increase the efficiency of the process and also relieve pressure on the mutual assistance system.

- Traffic data are also often sought in criminal investigations, and their rapid disclosure may be necessary for tracing the source of a communication as a starting point for collecting further evidence or to identify a suspect.
- Similarly, as many forms of crime online are facilitated by domains created or exploited for criminal purposes, it is necessary to identify the person who has registered such a domain. Such information is held by entities providing domain name registration services, that is, typically by registrars and registries. An efficient framework to obtain this information from relevant entities in other Parties is therefore needed.
- In an emergency situation, where there is a significant and imminent risk to the life or safety of any natural person, rapid action is needed either by providing for emergency mutual assistance or making use of the points of contact for the 24/7 Network established under the Convention (Article 35).
- In addition, proven international co-operation tools should be used more widely and between all Parties. Important measures, such as video conferencing or joint investigation teams, are already available under treaties of the Council of Europe (for example, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS No. 182) or other bilateral and multilateral agreements. However, such mechanisms are not universally available among Parties to the Convention, and this Protocol aims to fill that gap.
- The Convention provides for the collection and exchange of information and evidence for specific criminal investigations or proceedings. The drafters recognised that the establishment, implementation and application of powers and procedures related to criminal investigations and prosecutions must always be subject to conditions and safeguards that ensure adequate protection of human rights and fundamental freedoms. It was necessary, therefore, to include an article on conditions and safeguards, similar to Article 15 of the Convention. Furthermore, recognising the requirement in many Parties to protect privacy and personal data in order to meet their constitutional and international obligations, the drafters decided to provide for specific data protection safeguards in this Protocol. Such data protection safeguards complement the obligations of many of the Parties to the Convention, which are also

Parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). The amending protocol to that convention (CETS No. 223) was opened for signature during the drafting of this Protocol on October 2018. It should also be noted that the drafting process of this Protocol included Parties not subject, at the time, to Council of Europe instruments on data protection or to European Union data protection rules. Accordingly, significant efforts were undertaken to ensure a balanced Protocol reflective of the many legal systems of States likely to be Parties to this Protocol while respecting the importance of ensuring the protection of privacy and personal data as required by the constitutions and international obligations of other Parties to the Convention.

24. The drafters also considered other measures which, after thorough discussion, were not retained in this Protocol. Two of these provisions, namely, "undercover investigations by means of a computer system" and "extension of searches", were of high interest to the Parties but were found to require additional work, time and consultations with stakeholders, and were thus not considered feasible within the time frame set for the preparation of this Protocol. The drafters proposed that these be pursued in a different format and possibly in a separate legal instrument.

25. Overall, the drafters believed that the provisions of this Protocol would add much value both from an operational and from a policy perspective. This Protocol will significantly improve the ability of the Parties to enhance co-operation among the Parties and between Parties and service providers and other entities, and to obtain the disclosure of electronic evidence for the purpose of specific criminal investigations or proceedings. Thus, this Protocol, like the Convention, aims to increase the ability of law-enforcement authorities to counter cyber- and other crime, while fully respecting human rights and fundamental freedoms, and it emphasises the importance and value of an internet built on the free flow of information.

This Protocol

26. As stated in the preamble, this Protocol aims to further enhance co-operation on cybercrime and the ability of criminal justice authorities to collect evidence in electronic form of a criminal offence for the purpose of specific criminal investigations or proceedings through additional tools pertaining to more efficient mutual assistance and other forms of co-operation between competent authorities; co-operation in emergencies (that is, in situations

where there is a significant and imminent risk to the life or safety of any natural person); and direct co-operation between competent authorities and service providers and other entities in possession or control of pertinent information. The purpose of this Protocol, therefore, is to supplement the Convention and, as between the Parties thereto, the First Protocol.

27. This Protocol is divided into four chapters: I. "Common provisions"; II. "Measures for enhanced co-operation"; III. "Conditions and safeguards"; and IV. "Final provisions".

28. The common provisions of Chapter I cover the purpose and scope of this Protocol. As is the case for the Convention, this Protocol relates to specific criminal investigations or proceedings, not only with respect to cybercrime but any criminal offence involving evidence in electronic form also commonly referred to as "electronic evidence" or "digital evidence". This chapter also makes definitions of the Convention applicable to this Protocol and contains additional definitions of terms used frequently in this Protocol. Moreover, considering that language requirements for mutual assistance and other forms of co-operation often hinder the efficiency of procedures, an article on "language" was added to permit a more pragmatic approach in this respect.

29. Chapter II contains the primary substantive articles of this Protocol, which describe various methods of co-operation available to the Parties. Different principles apply to each type of co-operation. For this reason, it was necessary to divide this chapter into sections with (1) general principles applicable to Chapter II, (2) procedures enhancing direct co-operation with providers and entities in other Parties, (3) procedures enhancing international co-operation between authorities for the disclosure of stored computer data, (4) procedures pertaining to emergency mutual assistance and (5) procedures pertaining to international co-operation in the absence of applicable international agreements.

30. Chapter III provides for conditions and safeguards. They require that Parties shall apply conditions and safeguards similar to Article 15 of the Convention also to the powers and procedures of this Protocol. In addition, this chapter includes a detailed set of safeguards for the protection of personal data.

31. Most of the final provisions of Chapter IV are similar to standard final provisions of Council of Europe treaties or make provisions of the Convention applicable to this Protocol. However, Article 15 on "Effects of this Protocol", Article 17 on the "Federal clause" and Article 23 on the "Consultations of the Parties and assessment of implementation" differ in varying degrees from analogous provisions

of the Convention. This last article not only makes Article 46 of the Convention applicable but also provides that the effective use and implementation of the provisions of this Protocol shall be periodically assessed by the Parties.

Commentary on the articles of this Protocol

Chapter I – Common provisions

Article 1 – Purpose

32. The purpose of this Protocol is to supplement (i) the Convention as between the Parties to this Protocol, and (ii) the First Protocol as between the Parties thereto that are also Parties to this Protocol.

Article 2 – Scope of application

33. The general scope of application of this Protocol is the same as that of the Convention: the measures of this Protocol are to be applied, as between the Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data (that is, the offences covered by Article 14 of the Convention, paragraph 2.a and b), as well as to the collection of evidence in electronic form of a criminal offence (Article 14 of the Convention, paragraph 2.c). As explained in paragraphs 141 and 243 of the explanatory report to the Convention, this means that either where the crime is committed by use of a computer system, or where a crime not committed by use of a computer system (for example a murder) involves electronic evidence, the powers, procedures and co-operation measures created by this Protocol are intended to be available.

34. Paragraph 1.b states that as between Parties to the First Protocol that are also Parties to this Protocol, this Protocol also applies to specific criminal investigations or proceedings concerning the criminal offences established pursuant to the First Protocol. Parties to this Protocol that are not Parties to the First Protocol undertake no obligation to apply the terms of this Protocol to those offences.

35. Under paragraph 2, each Party is required to have a legal basis to carry out the obligations set forth in this Protocol if its treaties, laws or arrangements do not already contain such provisions. This does not change explicitly discretionary provisions into mandatory ones, and some provisions permit declarations or reservations. Some Parties may not require any implementing legislation in order to apply the provisions of this Protocol.

Article 3 – Definitions

36. Paragraph 1 incorporates the definitions provided in Articles 1 ("computer system", "computer data", "service provider" and "traffic data") and 18, paragraph 3 ("subscriber information"), of the Convention into this Protocol. The drafters included these definitions from the Convention because these terms are used in the operative text and explanatory report of this Protocol. The drafters also intended that explanations provided in the Convention's explanatory report and in guidance notes (adopted by the T-CY) related to those terms would equally apply to this Protocol.

37. The definitions of offences and of other terms included in the text of the Convention are intended to apply for purposes of co-operation between Parties to this Protocol, and the definitions of offences and of other terms included in the text of the First Protocol are intended to apply for purposes of co-operation between Parties to the First Protocol. For example, Article 2, paragraph 1, provides that "the measures described in this Protocol shall be applied … [a]s between Parties to the Convention that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data". Therefore, when co-operating under this Protocol with respect to offences related to child pornography, the definition of "child pornography" in Article 9, paragraph 2, of the Convention applies, and the definition of "minor" in Article 9, paragraph 3, of the Convention applies. Similarly, as between Parties to the First Protocol that are Parties to this Protocol, the definition of "racist and xenophobic material" in Article 2 of the First Protocol applies. Parties to this Protocol that are not Parties to the First Protocol undertake no obligation to apply the terms or definitions established in the First Protocol.

38. Paragraph 2 of Article 3 includes additional definitions that apply to this Protocol and co-operation under this Protocol. Paragraph 2.a defines "central authority" as the "authority or authorities designated under a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned, or, in the absence thereof, the authority or authorities designated by a Party under Article 27, paragraph 2.a, of the Convention". This Protocol uses central authorities in several articles in order to provide co-operation through a channel that Parties already use and are familiar with. Therefore, Parties that have mutual assistance treaties or arrangements on the basis of uniform or reciprocal legislation are required to use central authorities designated under those treaties or arrangements. Where no such treaty or arrangement is in place between the Parties concerned, those Parties are required to use the same central authority channel that they

currently use under Article 27, paragraph 2.a, of the Convention. Although not all mutual assistance treaties or arrangements on the basis of uniform or reciprocal legislation will use the term "central authority", the drafters intended this term to refer to the co-ordinating authorities designated in such treaties or arrangements, however denominated therein.

39. Unless specifically provided in this Protocol, the fact that Parties engage such central authority channels for the purpose of this Protocol does not mean that other provisions of those mutual assistance treaties or arrangements apply.

40. The definition of "competent authority" under paragraph 2.b is modelled on paragraph 138 of the explanatory report to the Convention. As this term is frequently used in this Protocol, the definition was placed in the operative text for ease of reference.

41. Paragraph 2.c defines "emergency" as "a situation in which there is a significant and imminent risk to the life or safety of any natural person". This term is used in Articles 9, 10 and 12. The definition of "emergency" in this Protocol is intended to impose a significantly higher threshold than "urgent circumstances" under Article 25, paragraph 3, of the Convention. This definition was also drafted to allow Parties to consider the different contexts in which the term is used in this Protocol while taking into account the Parties' applicable laws and policies.

42. The definition of emergency covers situations in which the risk is significant and imminent, meaning that it does not include situations in which the risk to the life or safety of the person has already passed or is insignificant, or in which there may be a future risk that is not imminent. The reason for these significance and imminence requirements is that Articles 9 and 10 place labour intensive obligations on both the requested and requesting Parties to react in a greatly accelerated manner in emergencies, which consequently requires that emergency requests be given a higher priority than other important but somewhat less urgent cases, even if they had been submitted earlier. Situations involving "a significant and imminent risk to the life or safety of any natural person" may involve, for example, hostage situations in which there is a credible risk of imminent loss of life, serious injury or other comparable harm to the victim; ongoing sexual abuse of a child; immediate post-terrorist attack scenarios in which authorities seek to determine with whom the attackers communicated in order to determine if further attacks are imminent; and threats to the security of critical infrastructure in which there is a significant and imminent risk to the life or safety of a natural person.

43. As explained in Article 10, paragraph 4, of this Protocol and in paragraph 154 of this explanatory report, which relates to Article 9, a requested Party under those articles will determine whether an "emergency" exists, applying the definition in this article.

44. Paragraph 2.d defines "personal data" as "information relating to an identified or identifiable natural person". An "identifiable natural person" is intended to refer to a person who can be identified, directly or indirectly, by reference to, in particular, an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. The definition of "personal data" under this Protocol is consistent with that in other international instruments, such as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as amended by its additional Protocol, the 2013 Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, the EU General Data Protection Regulation and Data Protection Law Enforcement Directive, and the African Union Convention on Cyber Security and Personal Data Protection ("Malabo Convention").

45. An individual is not considered "identifiable" if identification would require unreasonable time, effort or resources. While certain information may be unique to a particular individual, and thus establishes a link to that person in and by itself, other information may only allow identification when combined with additional personal or identifying information. Accordingly, if identification of an individual based on the connection to such additional information would require unreasonable time, effort or resources, the information at issue does not constitute personal data. Whether a natural person can be identified or is identifiable, directly or indirectly, depends on the particular circumstances in their specific context (and may change over time with technological or other developments).

46. The data protection requirements set out in this Protocol do not apply to data that are not "personal data", such as anonymised information that cannot be reidentified without unreasonable time, effort or resources.

Article 4 – Language

47. Article 4 provides a framework for languages that may be used when addressing Parties and service providers or other entities pursuant to this Protocol. Even where in practice Parties are able to work in languages other

than their official languages, such possibility may not be foreseen by domestic law or treaties. The objective of this article is to provide additional flexibility under this Protocol.

48. Inaccurate or costly translations of mutual assistance requests relating to electronic evidence are a chronic complaint requiring urgent attention. This impediment erodes legitimate processes to obtain data and protect public safety. The same considerations apply outside of traditional mutual assistance, such as when a Party transmits an order directly to a service provider in another Party's territory under Article 7, or requests to give effect to an order under Article 8. While machine translation capabilities are expected to improve, they are currently inadequate. For these reasons, the translation problem was mentioned repeatedly in proposals about articles to be included in this Protocol.

49. Translation to and from less-common languages is a special problem since such translations may greatly delay a request or may be effectively impossible to obtain. They may also be critically misleading, and their poor quality can waste the time of both Parties. However, the cost and difficulty of translations fall disproportionately on requesting Parties where less-common languages are spoken.

50. Because of this disproportionate burden, a number of non-Anglophone Parties asked that English be mandated in this Protocol. They noted that English is a commonly used language by major service providers. Furthermore, as data are moved and stored more widely in the world and more countries become involved in assisting each other, translation may become even more burdensome and impractical. For example, two Parties may use less-common languages, be geographically distant and have little contact. If Party A suddenly needs Party B's assistance, it may be unable to find a translator for B's language, or an eventual translation may be less intelligible than non-native English. The drafters particularly emphasised that, to speed up assistance, all efforts should be made to accept, in particular, emergency requests under this Protocol in English or a shared language rather than requiring translation into the official language of the requested Party.

51. The drafters of this Protocol concluded that English should not be mandated in this Protocol. Some Parties have official language requirements that preclude such a mandate; many Parties share a language and have no need for English; and, in some Parties, officials outside of capitals are less likely to be able to read English but are often involved in executing requests.

52. Thus, paragraph 1 is phrased in terms of "a language acceptable to the requested Party or the Party notified under Article 7". Such Party may specify acceptable languages – for example widely-spoken languages such as English, Spanish or French – even where those are not provided for in its domestic law or treaties.

53. As used in paragraph 1, "[r]equests, orders and accompanying information" refers to:

- under Article 8, the request (paragraph 3), the order (paragraph 3.a), the supporting information (paragraph 3.b) and any special procedural instructions (paragraph 3.c);
- for Parties that require notification under Article 7, paragraph 5, the order (paragraph 3), supplemental information (paragraph 4) and the summary of facts (paragraph 5.a);
- under Article 9, the request (paragraph 3).

"Requests" also refers to the contents of requests under Articles 10, 11 and 12 which includes documentation that is part of the request.

54. In practice, certain countries may be prepared to accept requests and orders in a language other than a language specified in domestic law or in treaties. Thus, once a year, the T-CY will engage in an informal survey of acceptable languages for requests and orders. Parties may alter their information at any time and all Parties will be made aware of any such change. They may state that they accept only specified languages for certain forms of assistance. The results of this survey will be visible to all Parties to the Convention, not merely Parties to this Protocol.

55. This pragmatic provision demonstrates the extreme importance of speeding up co-operation. It provides a treaty basis for a Party to accept additional languages for purposes of this Protocol.

56. In many cases, Parties have entered into mutual assistance treaties that specify the language or languages in which requests under those treaties must be submitted. This article does not interfere with the terms of those treaties or other agreements between Parties. Moreover, it is expected that for purposes of this Protocol, "a language acceptable to the requested Party or the Party notified under Article 7" would include any language or languages specified by those treaties or agreements. Therefore, a requesting Party should apply the language specified in mutual assistance treaties or other agreements to requests and notifications made under this Protocol, unless the requested

or notified Party indicates that it is also prepared to accept such requests or notification in other languages.

57. A Party's willingness to accept other languages will be reflected via its indication to the T-CY that it intends to accept some or all types of requests or notification of orders under this Protocol in another language.

58. Paragraph 2 determines the language(s) the issuing Party shall use to submit orders or requests and accompanying information to service providers or entities providing domain name registration services in another Party's territory pursuant to Articles 7 and 6 respectively. This provision is designed to ensure swift co-operation and increased certainty without imposing an additional burden on service providers or entities when they receive orders or requests to disclose data. The first option, provided in paragraph 2.a, indicates that the order or request can be submitted in a language in which the service provider or entity usually accepts domestic orders or requests from its own authorities in the framework of specific criminal investigations or proceedings ("comparable domestic process"). For Parties that have one or more official languages, this would include one of those languages. The second option, provided in paragraph 2.b, indicates that if a service provider or entity agrees to receive orders or requests in another language, for example the language of its headquarters, such orders and accompanying information can be submitted in that language. As a third option, paragraph 2.c provides that, when the order or request and accompanying information are not issued in one of the languages of the first two options, they shall be accompanied by a translation into one of those languages.

59. As used in paragraph 2, "[o]rders under Article 7 and requests under Article 6, and any accompanying information" refers to:

- under Article 6, the request (paragraph 3); and
- under Article 7, the order (paragraph 3) and the supplemental information (paragraph 4).

60. Where a Party has required notification pursuant to Article 7, a requesting Party must be prepared to send the order and any accompanying information in a language acceptable to the Party requiring notification, notwithstanding the acceptance by the service provider of other languages.

61. The T-CY will also informally endeavour to gather information on the languages in which orders and requests and accompanying information shall be submitted to service providers and entities providing domain name

registration services pursuant to Article 4, paragraph 2, and to make Parties aware of them as part of the survey described in paragraph 54 of the explanatory report, above.

Chapter II – Measures for enhanced co-operation

Section 1 – General principles applicable to Chapter II

Article 5 – General principles applicable to Chapter II

62. Paragraph 1 of Article 5 makes it clear that, as in Article 23 and Article 25, paragraph 1, of the Convention, Parties shall co-operate, in accordance with the provisions of Chapter II, "to the widest extent possible". This principle requires Parties to provide extensive co-operation and to minimise impediments to the smooth and rapid flow of information and evidence internationally.

63. Paragraphs 2 to 5 organise the seven co-operation measures of this Protocol into four different sections that follow the first section on general principles. These sections are divided by the types of co-operation sought: section 2 covers direct co-operation with private entities; section 3 contains forms of enhanced international co-operation between authorities for the disclosure of stored data; section 4 provides for mutual assistance in an emergency; and section 5 concludes with international co-operation provisions to be applied in the absence of a treaty or arrangement on the basis of uniform or reciprocal legislation between the Parties concerned. These sections are also organised roughly in a progression from the forms of investigatory assistance often sought early in an investigation – to obtain the disclosure of domain name registration and subscriber information – to requests for traffic data and then content data, followed by video conferencing and joint investigative teams, which are forms of assistance that are often sought in the later stages of an investigation.

64. This section on general principles makes clear the extent to which each measure is or is not affected by the existence of a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation between the Parties concerned, that is, the requesting Party and requested Party for government-to-government co-operation, and the Party seeking the information and the Party in whose territory the private entity in possession or control of such information is located for direct co-operation under Articles 6 and 7. An "arrangement on the basis of uniform or reciprocal legislation" is meant to refer to arrangements "such as the system of co-operation developed among the Nordic countries, which is also admitted by the European Convention on

Mutual Assistance in Criminal Matters (Article 25, paragraph 4), and among members of the Commonwealth" (see explanatory report, paragraph 263, to the Convention). The measures in sections 2 to 4 of this chapter apply whether or not the Parties concerned are mutually bound by an applicable mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation. The international co-operation provisions in section 5 apply only in the absence of such agreements or arrangements, except as provided otherwise.

65. As described in paragraph 2 of this article, section 2 of this chapter consists of Article 6, entitled "Request for domain name registration information", and Article 7, entitled "Disclosure of subscriber information". These are the so-called "direct co-operation" articles, which allow competent authorities of a Party to engage directly with private entities – that is, with entities providing domain name registration services in Article 6 and with service providers in Article 7 – for the purposes of specific criminal investigations or proceedings. Section 2 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Party seeking the information and the Party in whose territory the private entity in possession or control of such information is located.

66. As described in paragraph 3 of this article, section 3 of this chapter consists of Article 8, entitled "Giving effect to orders from another Party for expedited production of subscriber information and traffic data", and Article 9, entitled "Expedited disclosure of stored computer data in an emergency". These are measures "enhancing international co-operation between authorities", that is, it provides for co-operation between competent authorities, but of a different nature than traditional international co-operation. Section 3 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties.

67. As described in paragraph 4 of this article, section 4 of this chapter consists of Article 10, entitled "Emergency mutual assistance". Although emergency mutual assistance is a mutual assistance provision, it is an important co-operation tool for emergencies that is not expressly provided for in many mutual assistance treaties. Therefore, the drafters decided that this section should apply whether or not there is an applicable mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned. With respect to the procedures that govern emergency mutual assistance, there are two possibilities. When the Parties concerned are

mutually bound by an applicable mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, section 4 is supplemented by the provisions of that agreement unless the Parties concerned mutually determine to apply certain provisions of the Convention in lieu thereof (see Article 10, paragraph 8, of this Protocol). When the Parties concerned are not mutually bound by such agreement or arrangement, the Parties apply certain procedures set forth in Articles 27 and 28 of the Convention, concerning mutual assistance in the absence of a treaty (see Article 10, paragraph 7, of this Protocol).

68. As described in paragraph 5 of this article, section 5 of this chapter consists of Article 11, entitled "Video conferencing", and Article 12, entitled "Joint investigation teams and joint investigations". These provisions are measures of international co-operation, which apply only 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. These measures do not apply where such treaty or arrangement exists, except that Article 12, paragraph 7, applies whether or not such treaty or arrangement exists. However, the Parties concerned may mutually determine to apply the provisions of section 5 in lieu of such an existing treaty or arrangement unless this would be prohibited by the terms of the treaty or arrangement.

69. Paragraph 6 is modelled after Article 25, paragraph 5, of the Convention, and paragraph 259 of the explanatory report to the Convention is thus also valid here: "Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance … dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in denominating the offence. This provision was believed necessary in order to ensure that requested Parties do not adopt too rigid a test when applying dual criminality. Given differences in domestic legal systems, variations in terminology and categorisation of criminal conduct are bound to arise. If the conduct constitutes a criminal violation under both systems, such technical differences should not impede assistance. Rather, in matters in which the dual criminality standard is applicable, it should be applied in a flexible manner that will facilitate the granting of assistance."

70. Paragraph 7 provides that "[t]he provisions in this chapter do not restrict co-operation between Parties, or between Parties and service providers or other entities, through other applicable agreements, arrangements, practices

or domestic law". This means that the Protocol does not eliminate or restrict any co-operation between the Parties or between Parties and private entities that is otherwise available – whether through applicable agreements, arrangements, domestic law or even informal practices. The drafters intended to expand, not restrict, the tools available in the law-enforcement practitioner's toolbox to obtain information or evidence for specific criminal investigations or proceedings. The drafters recognised that in certain situations, existing mechanisms, such as mutual assistance, may be best for a practitioner to use. However, in other situations, the tools created by this Protocol may be more efficient or preferable. For instance, if a competent authority needs content data on a non-emergency basis, it would likely choose to use a traditional mutual assistance request under a bilateral treaty or under Article 27 of the Convention, as applicable, because the Protocol does not contain provisions for obtaining content data on a non-emergency basis. But if it needed subscriber information, it might choose to use Article 7 of the Protocol to issue an order directly to a service provider.

71. Finally, a number of provisions of Chapter II and elsewhere in this Protocol permit the imposition of use limitations or conditions, such as confidentiality. When, in accordance with the provisions of this Protocol, receipt of the evidence or information sought is subject to such a use limitation or condition, exceptions were recognised by the negotiators and are implicit in the text. First, as a measure for protecting human rights and liberties in accordance with Article 13, under the fundamental legal principles of many States, if material furnished to the receiving Party is considered by it to be exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. This principle is without prejudice to the text of Article 12, paragraph 6.b, and explanatory report, paragraph 215, that may be applied where Parties have established a joint investigation team. It was understood by the drafters that, in such cases, the receiving Party would notify the transferring Party prior to disclosure and, if so requested, consult with the transferring Party. Second, when a use limitation has been imposed with respect to material received under this Protocol that is foreseen for use at trial, the trial (including disclosures during pretrial judicial proceedings) is normally a public proceeding. Once made public at trial, the material has passed into the public domain. In these situations, it is not possible to ensure confidentiality to the investigation or proceeding for which the material was sought. These exceptions are similar to the exceptions related to the application of Article 28, paragraph 2, of the Convention as explained in paragraph 278 of the explanatory report to the Convention. Finally, material may be used for another purpose where the prior consent of a transferring Party has been obtained.

Section 2 – Procedures enhancing direct co-operation with providers and entities in other Parties

Article 6 – Request for domain name registration information

72. Article 6 establishes a procedure that provides for the direct co-operation between the authorities of one Party and an entity providing domain name registration services in the territory of another Party to obtain information about internet domain name registrations. Similar to Article 7, the procedure builds on the conclusions of the Cybercrime Convention Committee's Cloud Evidence Group, acknowledging the importance of timely cross-border access to electronic evidence in specific criminal investigations or proceedings, in view of the challenges posed by existing procedures for obtaining electronic evidence.

73. The procedure also acknowledges the current model of internet governance which relies on developing consensus-based multistakeholder policies. These policies are normally based on contractual law. The procedure set out in this article aims to complement those policies for the purposes of this Protocol, that is, for the purpose of specific criminal investigations or proceedings. Obtaining the domain name registration data is often indispensable, as a first step for many criminal investigations and to determine where to direct requests for international co-operation.

74. Many forms of cybercrime are facilitated by offenders creating and exploiting domains for malicious and illicit purposes. For example, a domain name may be used as a platform for the spreading of malware, botnets, phishing and similar activities, fraud, distribution of child abuse materials and for other criminal purposes. Access to information on the legal or natural person who registered a domain (the "registrant") is therefore critical to identify a suspect in a specific criminal investigation or proceeding. Whereas domain name registration data were historically publicly available, access to some of the information is now restricted, which affects judicial and law-enforcement authorities in their public policy tasks.

75. Domain name registration information is held by entities providing domain name registration services. These include organisations that sell domain names to the public ("registrars") as well as regional or national registry operators which keep authoritative databases ("registries") of all domain names registered for a top level domain and which accept registration requests. In certain cases, such information may be personal data and may be protected under data protection regulations in the Party where the respective entity providing domain name registration services (the registrar or registry) is located or where the person to whom the data relates is located.

76. The objective of Article 6 is to provide an effective and efficient framework to obtain information for identifying or contacting the registrant of a domain name. The form of implementation depends on the Parties' respective legal and policy considerations. This article is intended to complement current and future internet governance policies and practices.

Paragraph 1

77. Under paragraph 1, each Party shall adopt measures necessary to empower its competent authorities to issue requests directly to an entity providing domain name registration services in the territory of another Party, that is, without requiring the authorities in the territory where the entity is located to act as an intermediary. Paragraph 1 gives Parties flexibility regarding the format in which requests are made, since the format depends on the Parties' respective legal and policy considerations. A Party can use procedures available under its domestic law, including issuance of an order; however, for the purposes of Article 6, such an order is treated as a non-binding request. The form of the request or the effects it produces under the domestic law of the requesting Party would therefore not affect the voluntary nature of international co-operation under this article and, if the entity does not disclose the information sought, paragraph 5 would be applicable.

78. The wording in Article 6, paragraph 1, is sufficiently broad to acknowledge that such a request may also be issued and the information may be obtained via an interface, portal or other technical tool made available by organisations. For example, an organisation may provide an interface or lookup tool to facilitate or expedite the disclosure of domain name registration information following a request. However, rather than tailoring this article to any particular portal or interface, this article uses technology-neutral terms to permit adaptation to evolving technology.

79. As foreseen in Article 2, a request under paragraph 1 may be issued only for the purposes of specific criminal investigations or proceedings. The term "competent authority" is defined in Article 3, paragraph 2.b, and refers to a "judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under this Protocol". An "entity providing domain name registration services" currently refers to registrars and registries. To take the present situation into account and at the same time permit adaptation as business models and the architecture of the internet may change over time, this article uses the more generic term of an "entity providing domain name registration services".

80. While information for identifying or contacting the registrant of a domain name is often stored by entities providing general domain name registration services globally, for example "generic top level domains" (gTLDs), Parties acknowledged that more specific domain name registration services related to national or regional entities ("country-code top level domains" (ccTLDs)) may also be registered by persons or entities in other countries and may also be used by offenders. Therefore, Article 6 is not limited to entities providing gTLDs, as both types of domain name registration services – or future types of such services – can be used to perpetrate cybercrime.

81. The phrase "information for identifying or contacting the registrant of a domain name" refers to the information previously publicly available through so-called WHOIS lookup tools, such as the name, physical address, e-mail address and telephone number of a registrant. Some Parties may consider this information a subset of subscriber information as defined in Article 18, paragraph 3, of the Convention. Domain name registration information is basic information that would not permit precise conclusions to be drawn concerning the private lives and daily habits of individuals. Its disclosure may, therefore, be less intrusive than the disclosure of other categories of data.

Paragraph 2

82. Paragraph 2 requires each Party to adopt measures to permit entities in its territory providing domain name registration services to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law, which in some Parties may include data protection conditions. At the same time, Article 14 limits the ability to refuse data transfers under the data protection rules for international transfers, and the factors in paragraph 83 were included to facilitate processing under data protection rules. These measures should facilitate the disclosure of the requested data in a rapid and effective manner to the greatest extent possible.

83. This article does not require Parties to enact legislation obligating these entities to respond to a request from an authority of another Party. Thus, the entity offering domain name registration services may need to determine whether to disclose the information sought. This Protocol assists with this determination by providing safeguards that should facilitate the ability of entities to respond without difficulty to requests under this article, such as:

– this Protocol provides or requires Parties to provide a legal basis for requests;

- this article requires that the request emanate from a competent authority (Article 6, paragraphs 1 and 3.a, and paragraphs 79 and 84 of this explanatory report);
- this Protocol provides that a request is made for the purposes of specific criminal investigations or proceedings (Article 2);
- this article requires that the request contain a statement that the need for the information arises because of its relevance to a specific criminal investigation or proceeding and that the information will only be used for that specific criminal investigation or proceeding (Article 6, paragraph 3.c);
- this Protocol provides for safeguards for the processing of personal data disclosed and transferred pursuant to such requests through Article 14;
- the information to be disclosed is limited and would not permit precise conclusions to be drawn concerning the private lives of individuals;
- entities may be expected or required to co-operate under contractual arrangements with the Internet Corporation for Assigned Names and Numbers (ICANN).

Paragraph 3

84. Paragraph 3 of this article specifies the information that, at a minimum, shall be provided by an authority issuing a request pursuant to paragraph 1 of this article. This information is particularly relevant for the execution of the request by the entity providing domain name registration services. The request will need to include:

a. the date of the request and the identity and contact details of the competent authority issuing the request (paragraph 3.a) (see paragraph 79 of the explanatory report);

b. the domain name about which information is sought and a detailed list of the information sought, including the particular data elements such as the name, physical address, e-mail address or telephone number of a registrant (paragraph 3.b);

c. a statement that the request is issued pursuant to this Protocol; by making this statement the Party represents that the request is in accordance with the terms of this Protocol (paragraph 3.c). The requesting Party also confirms in this statement that the information is "need[ed]" because of its relevance to a specific criminal investigation or proceeding and that the information will only be used for that specific criminal investigation or proceeding. For European countries, what information is "need[ed]" – that is, necessary and

proportionate – for a criminal investigation or proceeding should be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence. Those sources stipulate that the power or procedure should be proportional to the nature and circumstances of an offence (see paragraph 146 of the explanatory report to the Convention on Cybercrime). Other Parties will apply related principles of their law, such as principles of relevance (that is, that the evidence sought by a request must be relevant to the investigation or prosecution). Parties should avoid broad requests for the disclosure of domain name information unless they are needed for the specific criminal investigation or proceeding;

d. the time and the manner in which to disclose the information and any other special procedural instructions (paragraph 3.d). "Special procedural instructions" is intended to include any request for confidentiality, including a request for non-disclosure of the request to the registrant or other third parties. If confidentiality is required to avoid a premature disclosure of the matter, this should be indicated in the request. In some Parties, confidentiality of the request will be maintained by operation of law, while in other Parties this is not necessarily the case. Therefore, where confidentiality is needed, Parties are encouraged to review publicly available information and to seek guidance from other Parties regarding applicable law, as well as the policies of the entities providing domain name registration services concerning subscriber/registrant information, prior to submitting a request under paragraph 1 to the entity. In addition, special procedural instructions may include specification of the transmission channel best suited to the authority's needs.

85. Paragraph 3 does not include a requirement to include a statement of facts in the request, considering that this information is confidential in most criminal investigations and may not be disclosed to a private party. However, the entity receiving a request under this article may need certain additional information that would allow it to come to a positive decision regarding the request. Therefore, the entity may seek other information where it cannot otherwise execute the request.

Paragraph 4

86. The goal of paragraph 4 is to encourage the use of electronic means when acceptable to the entity providing domain name registration services, as electronic means are nearly always the most efficient and fastest means of communication. Accordingly, if acceptable to the entity providing domain

name registration services, a Party may submit a request to the entity in electronic form, for example by using e-mail, electronic portals or other means. While it is assumed that entities prefer to receive requests in such format, it is not a requirement that this format only may be used. As foreseen in other articles of this Protocol permitting orders or requests in electronic form (such as Articles 7, 8 and others), appropriate levels of security and authentication may be required. The Parties and entities may decide themselves whether secure channels or means for transmission and authentication are available or whether special security protections (including encryption) may be necessary in a particular sensitive case.

Paragraph 5

87. While this provision pertains to "requests" and not to compulsory "orders" for the disclosure of domain name registration data, it is expected that a requested entity will be able to disclose the information sought pursuant to this provision where the applicable conditions have been met. If the entity does not disclose the requested information, other mechanisms to obtain the information could be considered, depending on the circumstances. Therefore, paragraph 5 provides for consultation between the Parties involved in order to obtain additional information and determine available mechanisms, for instance to improve future co-operation. In order to facilitate consultations, paragraph 5 also provides that a requesting Party may seek further information from an entity. Entities are encouraged to explain the reasons for not disclosing the data sought in response to such a request.

Paragraph 6

88. Paragraph 6 requires that, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, or at any other time, the Parties shall designate an authority for the purpose of consultation under paragraph 5. Providing a contact point in the Party where the entity is located will assist the requesting Party in quickly determining what measures are available to obtain the data sought, if the entity declines to execute a direct request made under Article 6.

Paragraph 7

89. Paragraph 7 is self-explanatory and provides that the Secretary General of the Council of Europe shall establish and maintain a register of the authorities designated under paragraph 6 and that each Party shall ensure that the details that it has provided for the register are correct at all times.

Article 7 – Disclosure of subscriber information

90. Article 7 establishes a procedure that provides for the direct co-operation between the authorities of one Party and a service provider in the territory of another Party to obtain subscriber information. The procedure builds on the conclusions of the T-CY's Cloud Evidence Group and Guidance Note on Article 18 of the Convention, acknowledging the importance of timely cross-border access to electronic evidence in specific criminal investigations or proceedings, in view of the challenges posed by existing procedures for obtaining electronic evidence from service providers in other countries.

91. An increasing number of criminal investigations or proceedings nowadays require access to electronic evidence from service providers in other countries. Even for crimes that are entirely domestic in nature – that is, where the crime, the victim and the perpetrator are all in the same country as the investigating authority – the electronic evidence may be held by a service provider in the territory of another country. In many situations, authorities that are investigating a crime may be required to use international co-operation procedures, such as mutual assistance, which are not always able to provide assistance rapidly or effectively enough for the needs of the investigation or proceeding due to the continually increasing volume of requests seeking electronic evidence.

92. Subscriber information is the most often sought information in criminal investigations relating to cybercrime and other types of crime for which electronic evidence is needed. It provides the identity of a particular subscriber to a service, his or her address, and similar information identified in Article 18, paragraph 3, of the Convention. It does not allow precise conclusions concerning the private lives and daily habits of individuals concerned, meaning that its disclosure may be of a lower degree of intrusiveness compared to the disclosure of other categories of data.

93. Subscriber information is defined in Article 18, paragraph 3, of the Convention (incorporated in Article 3, paragraph 1, of this Protocol) as "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service; b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. any other information on the site of the installation of communication equipment, available on the basis

of the service agreement or arrangement" (see also explanatory report to the Convention, paragraphs 177 to 183). Information needed for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time. In some Parties this information is treated as traffic data for various reasons, including that it is considered to relate to the transmission of a communication. Accordingly, paragraph 9.b of Article 7 provides a reservation for some Parties.

94. While Article 18 of the Convention already addresses some aspects of the need for rapid and effective access to electronic evidence from service providers, it does not in and of itself provide a complete solution to this challenge, since that article applies in a more limited set of circumstances. Specifically, Article 18 of the Convention applies when a service provider is "in the territory" of the issuing Party (see Article 18, paragraph 1.a, of the Convention) or "offering its services" in the issuing Party (see Article 18, paragraph 1.b of the Convention). Given the limits of Article 18 and the challenges facing mutual assistance, it was considered important to establish a complementary mechanism that would enable more effective cross-border access to information needed for specific criminal investigations or proceedings. Accordingly, the scope of Article 7 of this Protocol goes beyond the scope of Article 18 of the Convention by allowing a Party to issue certain orders to service providers in the territory of another Party. The Parties recognised that although such direct orders from authorities of one Party to service providers located in another Party are desirable for rapid and effective access to information, a Party should not be permitted to use all enforcement mechanisms available under its domestic law for enforcement of these orders. For that reason, enforcement of these orders in cases where the provider does not disclose the specified subscriber information is limited in the manner set forth in paragraph 7 of Article 7. This procedure provides for safeguards to take account of the unique requirements arising from a direct co-operation between authorities of one Party with service providers located in another Party.

95. As reflected in Article 5, paragraph 7, this article is without prejudice to the ability of Parties to enforce orders issued under Article 18 or otherwise as permitted by the Convention, nor does it prejudice co-operation (including spontaneous co-operation) between Parties, or between Parties and service providers, through other applicable agreements, arrangements, practices or domestic law.

Paragraph 1

96. Paragraph 1 requires Parties to provide competent authorities with the powers necessary to issue an order to a service provider in the territory of another Party to obtain disclosure of subscriber information. The order may only be issued for specified and stored subscriber information.

97. Paragraph 1 also includes the requirement that the orders may only be issued and submitted in the context of an issuing Party's own "specific criminal investigations or proceedings", as that phrase is used in Article 2 of this Protocol. As a further limitation, the orders may also only be issued for information that is "needed for" that investigation or proceeding. For European countries, what information is needed – that is, necessary and proportionate – for a criminal investigation or proceeding should be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence. Those sources stipulate that the power or procedure should be proportional to the nature and circumstances of an offence (see paragraph 146 of the explanatory report to the Convention). Other Parties will apply related principles of their law, such as principles of relevance (that is, that the evidence sought by an order must be relevant to the investigation or prosecution) and of avoiding overly broad orders for the disclosure of subscriber information. This restriction reemphasises the principle already set by Article 2 of this Protocol and paragraph 1 of Article 7, which limits the measure to specific criminal investigations and proceedings, that the provisions may not be used for mass or bulk production of data (see also paragraph 182 of the explanatory report to the Convention).

98. As defined in paragraph 2.b of Article 3, the term "competent authority" refers to a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of the measures under this Protocol. The same approach is foreseen for purposes of the direct co-operation procedure in this article. Accordingly, the domestic legal system of a Party will govern which authority is considered as a competent authority to issue an order. While the issuing Party determines which of its authorities may issue the order, Article 7 provides a safeguard in paragraph 5 whereby the receiving Party may require that a designated authority review the orders issued under this article and have the ability to halt direct co-operation, as described further below.

99. In Article 7, the term "a service provider in the territory of another Party" requires that the service provider be physically present in the other Party. Under this article, the mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being "in the territory" of that Party. Paragraph 1 requires, in addition, that the data be in the service provider's possession or control.

Paragraph 2

100. In paragraph 2 of Article 7, Parties are required to adopt any necessary measures for service providers in their territory to respond to an order issued by a competent authority in another Party pursuant to paragraph 1. Given the differences in domestic legal systems, Parties may implement different measures to establish a procedure for the direct co-operation to take place in an effective and efficient manner. This may range from removing legal obstacles for service providers to respond to an order to providing an affirmative basis, obliging service providers to respond to an order from an authority of another Party in an effective and efficient manner. Each Party must ensure that service providers can lawfully comply with orders foreseen by Article 7 in a manner that provides legal certainty so that service providers do not incur legal liability for the sole fact of having complied in good faith with an order issued under paragraph 1, which a Party has stated (under Article 7, paragraph 3.b) is issued pursuant to this Protocol. This does not preclude liability for reasons other than complying with the order, for example, failure to follow any applicable legal requirement that a service provider maintain appropriate levels of security of stored information. The form of implementation depends on Parties' respective legal and policy considerations. For Parties that have data protection requirements, this would include providing a clear basis for the processing of personal data. In view of additional requirements under data protection laws to authorise eventual international transfers of the responsive subscriber information, this Protocol reflects the important public interest of this direct co-operation measure and includes safeguards required for that purpose in Article 14.

101. As explained above, the domestic legal system of a Party will govern which authority is considered as a competent authority to issue an order. Some Parties felt it was necessary to have an additional safeguard of further review of the legality of the order (see, for example, paragraph 98 above) in light of the direct nature of the co-operation. While the issuing Party determines which of its authorities may issue the order, paragraph 2.b permits Parties to make

a declaration stating that "[t]he order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision". A Party making use of this declaration must accept an order by or under the supervision of any of these enumerated authorities.

Paragraph 3

102. Paragraph 3 of Article 7 specifies the information that, at a minimum, shall be provided by an authority issuing an order pursuant to paragraph 1 of this article, although an issuing Party may choose to include additional information in the order itself to assist in the processing or because its domestic law requires additional information. The information specified in paragraph 3 is particularly relevant for the execution of the order by the service provider, as well as the possible involvement of the authority of the Party wherein the service provider is located, pursuant to paragraph 5. The order will need to include the name of the issuing authority and the date the order was issued, information identifying the service provider, the offence that is the subject of the criminal investigation or proceeding, the authority seeking the subscriber information and a detailed description of the specific subscriber information sought. The order must also contain a statement that the order is issued pursuant to this Protocol. By making this statement, the Party represents that the order is in accordance with the terms of this Protocol.

103. Regarding the difference between paragraph 3.a (the issuing authority) and 3.e (the authority seeking the subscriber information), in some Parties, the issuing authority and the authority seeking the data are not the same. For instance, investigators or prosecutors may be the authorities seeking the data, while a judge issues the order. In such situations, both the authority seeking the data and the authority issuing the order must be identified.

104. No statement of facts is required, taking into account that this information is confidential in most criminal investigations and may not be disclosed to a private party.

Paragraph 4

105. While paragraph 3 sets out the minimum information required for orders issued pursuant to paragraph 1, these orders often can be executed only if the service provider (and, as applicable, the receiving Party's designated authority under paragraph 5) is provided with supplemental information. Therefore, paragraph 4 of Article 7 specifies that an issuing authority shall provide

supplemental information about the domestic legal grounds that empower the authority to issue the order; reference to legal provisions and applicable penalties for the offence being investigated or prosecuted; contact information of the authority to which the service provider shall return the subscriber information, request further information or otherwise respond; the time and the manner in which to return the subscriber information; whether preservation of the data has already been sought, including date of preservation and any applicable reference number; any special procedural instructions (for example requests for confidentiality or authentication); a statement, if applicable, that simultaneous notification has been made pursuant to paragraph 5; and any other information that may aid in obtaining disclosure of the subscriber information. Contact information need not identify the individual but only the office. This supplemental information can be provided separately but may also be included in the order itself if this is permissible under the issuing Party's law. Both the order and the supplemental information shall be transmitted directly to the service provider.

106. Special procedural instructions cover, in particular, any request for confidentiality, including a request for non-disclosure of the order to the subscriber or other third parties, except that special procedural instructions may not prevent the provider from consulting with authorities to be notified under paragraph 5.a or consulted with under paragraph 5.b. If confidentiality is required to avoid a premature disclosure of the matter, this should be indicated in the request. In some Parties, confidentiality of the order will be maintained by operation of law, while in other Parties this is not necessarily the case. Therefore, in order to avoid the risk of premature disclosure of the investigation, Parties are encouraged to be aware of applicable law and a service provider's policies concerning subscriber notification, prior to submitting the order under paragraph 1 to the service provider. In addition, special procedural instructions may include specification of the transmitting channel best suited to the authority's needs. The service provider may also request additional information regarding the account or other information to assist it in providing a prompt and complete response. A request for confidentiality should not prevent service providers from transparency reporting on anonymised aggregate numbers of orders received under Article 7.

Paragraph 5

107. Under paragraph 5.a, a Party may notify the Secretary General of the Council of Europe that, when an order is issued under paragraph 1 to a service provider in its territory, it will require simultaneous notification either in every

instance (that is, for all orders transmitted to service providers in its territory) or in identified circumstances.

108. Under paragraph 5.b, a Party may also, under its domestic law, require a service provider that receives an order from another Party to consult with it in identified circumstances. A Party may not require consultation for all orders, which would add an additional step that could cause significant delay, but only in more limited, identified circumstances. Consultation requirements should be limited to circumstances in which there is heightened potential for the need to impose a condition or to invoke a ground for refusal, or a concern of potential prejudice to the transferring Party's criminal investigations or proceedings.

109. The notification and consultation procedures are entirely discretionary. A Party is not obligated to require either procedure.

110. Parties notified under paragraph 5.a or consulted under paragraph 5.b may instruct a service provider not to disclose information on the grounds provided in paragraph 5.c which are described in more detail in paragraph 141 of the explanatory report on Article 8. Because of this, the ability of a Party to be notified or consulted provides an additional safeguard. That said, co-operation is in principle to be extensive and impediments thereto strictly limited. Accordingly, as explained in paragraphs 242 and 253 of the explanatory report to the Convention, the determination by the Party notified or consulted with as to which conditions and refusals would apply under Articles 25, paragraph 4, and 27, paragraph 4, of the Convention should also be limited in line with the objectives of Article 7 of the Protocol to eliminate barriers to and provide for more efficient and expedited procedures for cross-border access to electronic evidence for criminal investigations.

111. Under paragraph 5.d, the Parties that make a declaration under paragraph 5.a or that require consultation under paragraph 5.b may contact and seek additional information from the authority designated under paragraph 4.c in order to determine whether there is a basis under paragraph 5.c to instruct the service provider not to comply with the order. The process is intended to be as expeditious as circumstances will permit. The Party notified or consulted with must gather the necessary information and make their determination under paragraph 5.c "without undue delay". Where necessary, to enable co-operation, the procedure under paragraph 5.d may also provide an opportunity to clarify aspects of the confidentiality of the information sought, as well as any intended use limitation by the authority seeking the data. That Party must

also notify the issuing Party's authority promptly in the event that it decides to instruct the service provider not to comply, as well as provide the reasons for doing so.

112. A Party that requires notification or consultation may decide to impose on the provider a waiting period before the provider furnishes the subscriber information in response to the order, in order to permit notification or consultation and any follow-up request by the Party for additional information.

113. Pursuant to paragraph 5.e, a Party requiring notification or consultation must designate a single authority and, when notification is required under paragraph 5.a, provide the Secretary General of the Council of Europe with adequate contact information.

114. A Party may change its notification or its consultation requirement at any time, depending on its determination of any factors that are relevant to it, such as, for example, whether it wishes to move from a notification regime to a consultation regime or whether it has developed a sufficient comfort level with direct co-operation that it can revise or remove a previous notification or consultation requirement. It can equally decide that, as a result of experience it has gained with the direct co-operation mechanism, it wishes to institute a notification or consultation regime.

115. Under paragraph 5.f, the Secretary General of the Council of Europe is required to set up and keep current a register of the Parties' notification requirements under paragraphs 5.a and 5.e. Having an up-to-date register publicly available is critical to ensuring that the issuing Party's authorities and service providers are aware of each Party's notification requirements, which, as stated above, can change at any time. Since each Party may make such a change at its discretion, each Party that makes any change or notes any inaccuracy regarding its details in the register is required to notify the Secretary General immediately in order to ensure that others are aware of the current requirements and can properly apply them.

Paragraph 6

116. Paragraph 6 makes clear that notifying another Party and providing additional information using electronic means, including use of e-mail and electronic portals, is permissible. If acceptable to the service provider, a Party may submit an order under paragraph 1 and supplemental information under paragraph 4 in electronic form. The goal is to encourage the use of electronic means if acceptable to the service provider, as these are nearly always the most efficient

and fastest means of communication. Authentication methods may include a variety of means or a combination thereof allowing a secure identification of the requesting authority. Such means may include, for example, obtaining confirmation of authenticity via a known authority in the issuing Party (for example from the sender or a central or designated authority), subsequent communications between the issuing authority and receiving Party, use of an official e-mail address or future technological verification methods that can be easily used by transmitting authorities. A similar text is set forth in paragraph 2 of Article 10, and further guidance with respect to the security requirement is provided in paragraph 174 of the explanatory report. Article 6, paragraph 4, and Article 8, paragraph 5, of the Protocol also contain similar text.

Paragraph 7

117. Paragraph 7 provides that, if a service provider does not comply with an order issued under Article 7, the issuing Party may only seek enforcement pursuant to Article 8 or another form of mutual assistance. Parties proceeding under this article may not seek unilateral enforcement.

118. For enforcement of the order via Article 8, this Protocol contemplates a simplified procedure of conversion of an order under this article to an order under Article 8 to facilitate the ability of the issuing Party to obtain subscriber information.

119. In order to avoid duplication of efforts, an issuing Party must give the service provider 30 days or the time frame stipulated in paragraph 4.d, whichever time period is longer, for the notification and consultation process to occur and for the service provider to disclose the information or indicate a refusal to do so. Only after that time period has expired, or if the provider has indicated a refusal to comply before that time period has expired, may an issuing Party seek enforcement pursuant to Article 8 or other forms of mutual assistance. In order to allow authorities to assess whether to seek enforcement under paragraph 7, service providers are encouraged to explain the reasons for not providing the data sought. For example, a service provider may explain that the data are no longer available.

120. If an authority notified under paragraph 5.a or consulted with under paragraph 5.b has informed the issuing Party that the service provider has been instructed not to disclose the information sought, the issuing Party may nonetheless seek enforcement of the order via Article 8 or another form of mutual assistance. However, there is a risk that such a further request may likewise be denied. The issuing Party is advised to consult in advance with

an authority designated under paragraphs 5.a or 5.b in order to address any deficiencies in the original order and to avoid submitting orders under Article 8 or via any other mutual assistance mechanism that may be rejected.

Paragraph 8

121. Under paragraph 8, a Party may declare that another Party shall seek disclosure of subscriber information from the service provider before seeking it under Article 8 unless the issuing Party provides reasonable explanation for not having done so. For example, a Party may make such a declaration because it considers that the procedures under this article should enable other Parties to obtain the subscriber data more quickly than under Article 8, and, as a result, could reduce the number of situations in which Article 8 needs to be invoked. Article 8 procedures would then only be used when efforts to seek disclosure of subscriber information directly from the service provider were unsuccessful, when the issuing Party has a reasonable explanation for not first using this article or when the issuing Party has reserved the right not to apply this article. For instance, an issuing Party may demonstrate this when a service provider routinely does not provide subscriber information in response to orders received directly from that Party. Or, as another example, if an issuing Party through a single order seeks both subscriber information and traffic data from another Party that applies Article 8 to both categories of data, the issuing Party would not need to first seek the subscriber information separately.

Paragraph 9

122. Under paragraph 9.a, a Party that reserves to this article is not required to take measures under paragraph 2 for service providers in its territory to disclose subscriber information in response to orders issued by other Parties. A Party that reserves to this article is not permitted to issue orders under paragraph 1 to service providers in other Parties' territories.

123. Paragraph 9.b provides that – for the reasons explained in paragraph 93 above – if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system, a Party may reserve the right not to apply this article to such numbers. A Party that makes such a reservation is not permitted to issue orders for such numbers under paragraph 1 to service providers in other Parties' territories.

Section 3 – Procedures enhancing international co-operation between authorities for the disclosure of stored computer data

Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data

124. The purpose of Article 8 is for a requesting Party to have the ability to issue an order to be submitted as part of a request to another Party and for the requested Party to have the ability to give effect to that order by compelling a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control.

125. This article establishes a mechanism that complements the mutual assistance provisions of the Convention. It is designed to be more streamlined than mutual assistance currently is, in that the information the requesting Party must provide is more limited and the process for obtaining the data more rapid. This article complements, and therefore is without prejudice to, other mutual assistance processes under the Convention, or other multilateral or bilateral agreements, which a Party remains free to invoke. Indeed, in situations in which a requesting Party wishes to seek traffic data from a Party that has reserved to that aspect of Article 8, the requesting Party can use another mutual assistance procedure. Where, as is often the case, subscriber information, traffic data and stored content data are sought at the same time, it may be more efficient to seek all three forms of data for the same account via a single traditional mutual assistance request, rather than to seek some types of data via the method provided by this article and others via a separate mutual assistance request.

Paragraph 1

126. Paragraph 1 requires that the requesting Party be able to issue an order to obtain subscriber information or traffic data from a service provider in another Party's territory. The "order" referred to in Article 8 is any legal process that is intended to compel a service provider to provide subscriber information or traffic data. For example, it can be implemented by a production order, a subpoena or other mechanism that is authorised in law and that can be issued for the purpose of compelling the production of subscriber information or traffic data.

127. As defined in paragraph 2.b. of Article 3, "competent authority" in paragraph 1 of this article refers to a "judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or

undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings". It should be noted that the authorities competent to issue an order under paragraph 1 may not necessarily be the same as the authorities designated to submit the order to be given effect in accordance with paragraph 10.a of Article 8, as described in greater detail below.

128. Article 8, the term "a service provider in the territory of another Party" requires that the service provider be physically present in the other Party. Under this article, the mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being "in the territory" of that Party. Paragraph 1 requires, in addition, that the data be in the service provider's possession or control.

Paragraph 2

129. Paragraph 2 requires the requested Party to adopt measures necessary to give effect in its territory to an order issued under paragraph 1, subject to the safeguards described further below. "Giving effect" means that the requested Party would compel the service provider to provide the subscriber information and traffic data using the mechanism of the requested Party's choice, provided that the mechanism makes the order enforceable under the requested Party's domestic law and meets the requirements of this article. For example, a requested Party may give effect to a requesting Party's order by accepting it as equivalent to domestic orders, by endorsing it to give it the same effect as a domestic order or by issuing its own production order. Any such mechanism will be subject to the terms of the law of the requested Party, since the requested Party's procedures will control it. Therefore, the requested Party can ensure that its own law, including constitutional and human rights requirements, is satisfied, especially in relation to any additional safeguards including those necessary for the production of traffic data.

130. While this article can be complied with in a number of ways, a Party may wish to design its own internal processes with the flexibility to handle requests from the variety of competent authorities. Paragraph 3.b was negotiated to ensure that sufficient information was provided to the requested Party to ensure that a full review could take place if needed, as some Parties indicated that they would be issuing their own order as a way of giving effect to the requesting Party's order.

Paragraph 3

131. To initiate the requested Party's process to give effect to the order, the requesting Party shall transmit the order and supporting information. Paragraph 3 describes what a requesting Party must provide to the requested Party in order for the requested Party to give effect to the order and compel production from a service provider in that Party's territory. Paragraph 3.a describes information to be included in the order itself and includes information that is fundamental to its execution. The information in paragraph 3.b, which is for the use of the requested Party only and not to be shared with the service provider except with the consent of the requesting Party, is supporting information that establishes the domestic legal grounds and international basis in this Protocol for the order, and provides information for the requested Party to evaluate potential grounds for conditions or refusal under paragraph 8. Parties should, at the time they initiate a request under Article 8, indicate if there is any information under paragraph 3.b that may be shared with the service provider. Under paragraph 3.c, the request should also include all special instructions, including, for example, requests for certification or confidentiality of the request (similar to Article 27, paragraph 8, of the Convention), at the time of transmission to ensure the proper processing of the request.

132. The order for subscriber information or traffic data described in paragraph 3.a must, on its face, specify: (i) the authority that issued the order and the date the order was issued; (ii) a statement that it is being issued pursuant to this Protocol; (iii) the name and address of the service provider(s) to be served; (iv) the offence(s) that is/are the subject of the criminal investigation or proceeding; (v) the authority seeking the data, if not the issuing authority; and (vi) a detailed description of the specific data sought (that is the subscriber's identity, postal or geographic address, telephone or other access number, and billing and payment information available on the basis of the service agreement or arrangement (see Article 3 of this Protocol incorporating Article 18, paragraph 3, of the Convention and explanatory report paragraph 93 above); and in relation to traffic data, 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 (see Article 3, paragraph 1 of this Protocol incorporating Article 1, paragraph d, of the Convention)). With regard to paragraph 3.a.v, if the issuing authority and the authority seeking the data are not the same, the provision requires both to be identified. For instance, an investigating or prosecuting authority may be

seeking the data, while a judge issues the order. This information demonstrates the legitimacy of the order and provides clear instructions for its execution.

133. The supporting information described in paragraph 3.b is intended to provide the requested Party with information it would need to give effect to the requesting Party's order. This could also be facilitated by a template that would be easy to fill out, which could further add efficiency to the process. Included in the list of supporting information are the following:

- Paragraph 3.b.i refers to the statutory basis that gives the issuing authority the power to issue the order to compel production. In other words, this is the relevant law that empowers a competent authority to issue the order described in paragraph 1.
- Paragraph 3.b.ii refers to the legal provision relating to the offence referenced in the order at paragraph 3.a.iv and its associated range of penalties. The inclusion of both these elements is important for the requested Party to assess whether or not the request is within the scope of its obligations.
- Paragraph 3.b.iii refers to any information that the requesting Party can provide that led it to conclude that the service provider(s) which is the subject of the order is in possession or control of the information or data sought. This information is key to initiating the process in the requested Party. Identification of the domestic service provider and belief that it possesses or controls the information or data sought is often a prerequisite for initiating production order applications.
- Paragraph 3.b.iv refers to a brief summary of the facts related to the investigation or proceeding. This information is also a key factor for the requested Party to determine whether or not an order under this article should be given effect in its territory.
- Paragraph 3.b.v refers to a statement regarding the relevance of the information or data to the investigation or proceeding. This statement is to help the requested Party to decide whether or not the requirements of paragraph 1 of this article have been met, that is, that the information or data are "needed for the Party's specific criminal investigations or proceedings".
- Paragraph 3.b.vi refers to the contact information of an authority or authorities in case the competent authority in the requested Party requires additional information for giving effect to the order.

– Paragraph 3.b.vii refers to information as to whether preservation of the information or data has already been sought. This is important information for the requested Party, especially in relation to traffic data and should include, for example, reference numbers and date of preservation, as this information may permit the requested Party to match the current request to a previous preservation request and, thereby, facilitate disclosing the information or data originally preserved. In order to reduce the risk that information or data are deleted, Parties are encouraged to seek preservation of the information or data sought as soon as possible and prior to initiating a request under this article, and to seek extension of preservations in a timely manner.
– Paragraph 3.b.viii refers to information as to whether the data have already been sought by other means and, if so, in what manner. This provision addresses primarily whether the requesting Party has already sought subscriber information or traffic data directly from the service provider.

134. The information to be provided pursuant to paragraph 3.b shall not be disclosed to the service provider without the consent of the requesting Party. In particular, the summary of the facts and statement regarding the relevance of the information or data to the investigation or proceeding is provided to the requested Party for the purpose of determining whether there is a ground for imposing terms or conditions or for refusal, but is often subject to the secrecy of the investigation.

135. Under paragraph 3.c, the requesting Party may request special procedural instructions, including requests for non-disclosure of the order to the subscriber or authentication forms to be completed for the evidence. This information will have to be known at the outset, as special instructions may require additional processes within the requested Party.

136. To give effect to the order and further facilitate the production of the information or data, the requested Party may provide the service provider with additional information, such as the method of production, and to whom the data should be produced in the requested Party.

Paragraph 4

137. Pursuant to paragraph 4, additional information may need to be provided to the requested Party in order for it to give effect to the order. For example, under some Parties' domestic law, the production of traffic data may require further information because there are additional requirements in their laws

for obtaining such data. In addition, the requested Party may seek clarification regarding information provided pursuant to paragraph 3.b. As another example, some Parties may require additional information where the order was not issued or reviewed by a prosecutor or other judicial or independent administrative authority of the requesting Party. When making such a declaration, Parties should be as specific as possible with regard to the type of further information required.

Paragraph 5

138. Paragraph 5 requires the requested Party to accept requests in electronic form. It may require the use of secure and authenticatable means of electronic communications to facilitate the transmission of information or data and documents, including transmission of orders and supporting information. Articles 6 to 11 also foresee such means of communication.

Paragraph 6

139. Under paragraph 6, the requested Party should take reasonable steps to proceed expeditiously with respect to the request. It shall make reasonable efforts to process requests and have the service provider served within forty-five days after the requested Party has received all the necessary documents and information. The requested Party shall order the service provider to produce the subscriber information within twenty days and traffic data within forty-five days. While the requested Party should seek to compel production as expeditiously as possible, there are many factors that may delay production, such as service providers objecting, not responding to requests or not meeting the return date for production, as well as the volume of requests a requested Party may be asked to process. Because of this, it was decided to require requested Parties to make reasonable efforts to complete only the processes under their control.

Paragraph 7

140. The Parties acknowledged that some special procedural instructions from the requesting Party may also cause delays in the processing of orders, if the instructions require additional domestic processes in order to give effect to the special procedural instructions. The requested Party may also require additional information from the requesting Party in order to support any applications for supplementary orders, such as confidentiality orders (non-disclosure orders). Some procedural instructions may not be available under the requested Party's law, in which case paragraph 7 provides that it

shall promptly inform the requesting Party and specify any conditions under which it could comply, giving the requesting Party the ability to determine whether or not it wishes to continue with the request.

Paragraph 8

141. Under paragraph 8, the requested Party may refuse to execute a request if the grounds for refusal established in Articles 25, paragraph 4, or 27, paragraph 4, of the Convention exist. For example, in line with paragraph 257 of the explanatory report to the Convention, this provides that this provision is subject to the grounds for refusal in applicable mutual assistance treaties and domestic laws and provides "safeguards for the rights of persons located in the requested Party", and, in line with paragraph 268 of that explanatory report, assistance may be refused on the grounds of "prejudice to the sovereignty of the State, security, *ordre public* or other essential interests". It may also impose conditions necessary to permit execution of the request, such as confidentiality. In addition, the requested Party may postpone execution of the request under Article 27, paragraph 5, of the Convention. The requested Party shall notify the requesting Party of its decision to refuse, condition or postpone the request. In addition, Parties may apply use limitation in accordance with the terms of Article 28, paragraph 2.b, of the Convention.

142. In order to promote the principle of providing the widest measure of co-operation (see Article 5, paragraph 1), grounds for refusal established by a requested Party should be narrow and exercised with restraint. It should be recalled that the paragraph 253 of the explanatory report to the Convention provides that "mutual assistance is in principle to be extensive, and impediments thereto strictly limited". Accordingly, conditions and refusals should also be limited in line with the objectives of this article to eliminate barriers to transborder sharing of subscriber information and traffic data, and to provide more efficient and expedited procedures than traditional mutual assistance.

Paragraph 9

143. Under paragraph 9, "[i]f a requesting Party cannot comply with a condition imposed by the requested Party under paragraph 8, it shall promptly inform the requested Party. The requested Party shall then determine if the information or material should nevertheless be provided. … If the requesting Party accepts the condition, it shall be bound by it. The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain, in relation to that condition, the use made of such information or material".

Paragraph 10

144. The purpose of paragraph 10 is to ensure that Parties, at the time of signature, or when depositing their instruments of ratification, acceptance or approval, identify the authorities to submit and receive orders under Article 8. Parties need not give the name and address of a specific individual but may identify an office or unit that has been deemed competent for the purposes of sending and receiving orders under this article.

Paragraph 11

145. Paragraph 11 permits a Party to declare that it requires that orders submitted to it under this article be transmitted by the central authority of the requesting Party, or other authority where mutually determined between the Parties. Parties are encouraged to provide as much flexibility as possible for the submission of requests.

Paragraph 12

146. Paragraph 12 requires the Secretary General of the Council of Europe to set up and keep updated a register of the authorities designated by the Parties under paragraph 10 and for each Party to ensure that its details held on the register are accurate. Such information will assist requested Parties to verify the authenticity of requests.

Paragraph 13

147. Under paragraph 13, a Party that reserves the right not to apply this article to traffic data is not required to give effect to orders for traffic data from another Party. A Party that reserves to this article is not permitted to submit orders for traffic data to other Parties under paragraph 1.

Article 9 – Expedited disclosure of stored computer data in an emergency

148. In addition to the other forms of expedited co-operation provided for in this Protocol, the drafters were conscious of the need to facilitate Parties' ability, in an emergency, to expeditiously obtain specified stored computer data in the possession or control of a service provider in another Party's territory for use in specific criminal investigations or proceedings. As stated in paragraphs 42 and 172 of this explanatory report, the need for maximum expedited co-operation may arise in a variety of emergency situations, such as in the immediate aftermath of a terrorist attack, a ransomware attack that

may cripple a hospital system, or when investigating e-mail accounts used by kidnappers to issue demands and communicate with the victim's family.

149. Under the Convention, in an emergency, Parties make mutual assistance requests to obtain data and, under Article 35, paragraph 1.c, of the Convention, the 24/7 Network is available to facilitate the execution of such requests. In addition, a few countries' legal systems permit competent authorities of other countries to seek emergency disclosure of data via the 24/7 Network without sending a mutual assistance request.

150. As reflected in Article 5, paragraph 7, this article does not prejudice co-operation (including spontaneous co-operation) between Parties, or between Parties and service providers, through other applicable agreements, arrangements, practices or domestic law. Therefore, under this Protocol, all of the above mechanisms remain available to competent authorities that seek data in an emergency. The innovation of this Protocol is the elaboration of two articles that obligate all Parties to provide, at a minimum, specific channels for rapidly expedited co-operation in emergency situations: Article 9 and Article 10.

151. This article permits Parties to co-operate to obtain computer data in emergency situations using as a channel the 24/7 Network established by Article 35 of the Convention. The 24/7 Network is particularly well suited for handling the time-sensitive and high priority requests envisioned under this article. The 24/7 Network is staffed with points of contact who, in practice, communicate rapidly and without the need for written translations and are in a position to effectuate requests received from other Parties, whether by going directly to providers in their territory, soliciting assistance from other competent authorities or going to judicial authorities, should that be required under the Party's domestic law. These points of contact can also advise requesting Parties on questions they might have regarding providers and electronic evidence collection, for example by explaining the domestic law that must be satisfied to obtain evidence. Such back-and-forth communication enhances the requesting Party's understanding of the domestic law in the requested Party and facilitates smoother acquisition of needed evidence.

152. Using the channel established in this article may have advantages over the emergency mutual assistance channel set forth in Article 10. For example, this channel has the advantage that no mutual assistance request need be prepared in advance. Considerable time may be needed to prepare a prior mutual assistance request, have it translated and pass it through domestic channels to the requesting Party's central authority for mutual assistance, which

would not be required under Article 9. In addition, once the requested Party has received the request, if it must obtain supplemental information before it can grant assistance, the additional time that may be needed for a mutual assistance request is more likely to slow execution of the request. In the mutual assistance context, requested Parties often require that the supplemental information be provided in a written and more detailed form, whereas the 24/7 channel operates using real-time exchange of information. On the other hand, the emergency mutual assistance channel offers advantages in certain situations. For example, (i) little or no time may be lost by using that channel if there are particularly close working relations between the central authorities concerned; (ii) emergency mutual assistance may be used to obtain additional forms of co-operation beyond computer data held by providers; and (iii) it may be easier to authenticate evidence obtained via mutual assistance. It is up to the Parties, based on their accumulated experience and the specific legal and factual circumstances at hand, to decide which is the best channel to use in a particular case.

Paragraph 1

153. Under paragraph 1.a, each Party shall adopt measures as necessary to ensure that its point of contact for the 24/7 Network is able to transmit requests in an emergency to the point of contact in another Party, requesting immediate assistance with obtaining the expedited disclosure of specified, stored computer data held by providers in the territory of that Party and to receive requests from points of contact in other Parties for such data held by providers in its territory. As provided for in Article 2 the request must be made pursuant to a specific criminal investigation or proceeding.

154. The 24/7 points of contact must have the ability to transmit and receive such requests in an emergency without a request for mutual assistance having to be prepared and transmitted in advance, as described in paragraph 152 of the explanatory report above, subject to the possibility of a declaration under Article 9, paragraph 5. The term "emergency" is defined in Article 3. Under the Article 9, the requested Party should determine whether an "emergency" exists in relation to a request using the information provided in paragraph 3.

155. As opposed to other articles in this Protocol, such as Article 7, which may only be used to obtain "specified, stored subscriber information", this article uses the broader term "specified, stored computer data". The scope of this term is broad but not indiscriminate: it covers any "specified" computer data as defined in Article 1.b of the Convention, which is incorporated in Article 3,

paragraph 1, of this Protocol. The use of this broader term recognises the importance of obtaining stored content and traffic data, and not only subscriber information, in emergency situations, without requiring the submission of a request for mutual assistance as a prerequisite. The data in question are stored or existing data and do not include data that have not yet come into existence, such as traffic data or content data related to future communications (see paragraph 170 of the explanatory report to the Convention).

156. This provision provides flexibility to the requesting Party to determine which of its authorities should initiate the request, such as its competent authorities that are conducting the investigation or its 24/7 point of contact, in accordance with domestic law. The 24/7 Network point of contact in the requesting Party then operates as the channel to transmit the request to the 24/7 point of contact in the other Party.

157. Under paragraph 1.b, a Party may declare that it will not execute a request under Article 9 only for subscriber information, as defined in Article 18.3 of the Convention, incorporated in Article 3, paragraph 1, of this Protocol. For some Parties, receiving requests under this article solely for subscriber information would risk overburdening 24/7 Network points of contact by diverting resources and energy away from requests for content or traffic data. In such cases, Parties seeking only subscriber information may instead use Articles 7 or 8, which facilitate the rapid disclosure of such information. Such a declaration does not prohibit other Parties from including a request for subscriber information when they are also issuing a request under this article for content and/or traffic data.

Paragraph 2

158. Paragraph 2 requires that each Party adopt measures as necessary to ensure that its authorities are enabled under its domestic law to seek and obtain data requested under paragraph 1 from service providers in its territory, and to respond to such requests without the requesting Party having to submit a request for mutual assistance, subject to the possibility to make a declaration in accordance with paragraph 5.

159. Given the difference in national laws, paragraph 2 is designed to provide flexibility for Parties in constructing their systems for responding to requests under paragraph 1. Parties are encouraged, however, to develop mechanisms for complying with this article that emphasise speed and efficiency, that are adapted to the exigencies of an emergency situation and that provide a broad legal basis for disclosure of data to other Parties in emergency situations.

160. It is within the discretion of the requested Party to determine: (i) whether the requirements for use of this article have been met; (ii) whether another mechanism is suitable for the purposes of assisting the requesting Party; (iii) the appropriate authority to execute a request received by the 24/7 Network point of contact. While the 24/7 Network point of contact in some Parties may already have the requisite authority to execute the request itself, other Parties may require that their point of contact forward the request to another authority or authorities to seek disclosure of the data from the provider. In some Parties, this may require the obtaining of a judicial order to seek disclosure of data. The requested Party also has discretion to determine the channel for transmitting the responsive data to the requesting Party – whether through the 24/7 point of contact or through another authority.

Paragraph 3

161. Paragraph 3 specifies the information to be provided in a request pursuant to paragraph 1. The information specified in paragraph 3 is to facilitate the review and, where appropriate, execution of the request by the relevant authority of the requested Party.

162. With regard to paragraph 3.a, the requesting Party shall specify the competent authority on whose behalf the data are sought.

163. With regard to paragraph 3.b, the requesting Party must state that the request is issued pursuant to this Protocol. This will provide assurance that the request is made consistent with this Protocol and that any data received as a result will be handled in a manner consistent with the requirements of this Protocol. This will also differentiate the request from other emergency disclosure requests the 24/7 Network point of contact might receive.

164. Under paragraph 3.e, the requesting Party must provide sufficient facts that demonstrate the existence of an emergency, as defined in Article 3, and how the data sought by the request relates to that emergency. Should the requested Party require clarification of the request or require additional information to act on the request, it should consult with the requesting Party's 24/7 Network point of contact.

165. Under paragraph 3.g, the request shall specify any special procedural instructions. These include, in particular, requests for non-disclosure of the request to subscribers and other third parties or authentication forms to be completed for the data sought. Under this paragraph, these procedural instructions are provided at the outset, as special instructions may require additional processes

within the requested Party. In some Parties, confidentiality may be maintained by operation of law while, in other Parties, this is not necessarily the case. Therefore, in order to avoid the risk of premature disclosure of the investigation, Parties are encouraged to communicate regarding the need for and any difficulties that may arise in maintaining confidentiality, including any applicable law, as well as a service provider's policies concerning notification. Since requests for authentication of the responsive data can often slow the key objective of rapid disclosure of the data sought, the authorities of the requested Party should, in consultation with the authorities of the requesting Party, determine when and in what manner confirmation of authenticity should be provided.

166. In addition, the Party or service provider may require additional information to locate and disclose the stored computer data sought by the requesting Party.

Paragraph 4

167. Paragraph 4 requires the requested Party to accept requests in electronic form. Parties are encouraged to use rapid means of communication to facilitate the transmission of information or data and documents, including transmission of requests. This paragraph is based on paragraph 5 of Article 8 but it has been modified to add that a Party may accept requests orally, a method of communication frequently used by the 24/7 Network.

Paragraph 5

168. Paragraph 5 permits a Party to make a declaration that it requires other Parties that request data from it pursuant to this article to provide, following the execution of the request and transmission of the data, the request and any supplemental information transmitted in support thereof, in a specific format and through a specific channel. For instance, a Party may declare that in specific circumstances, it will require that a requesting Party submit a subsequent mutual assistance request in order to formally document the emergency request and the prior decision to provide data in response to such a request. For some Parties such a procedure would be required by their domestic law, whereas other Parties indicated that they have no such requirements and do not need to avail themselves of this possibility for a declaration.

Paragraph 6

169. This article refers to "requests" and does not require requested Parties to provide requested data to requesting Parties. Therefore, the drafters acknowledge that there will be situations in which requested Parties will not provide

requested data to a requesting Party under this article. The requested Party may determine that, in a particular case, emergency mutual assistance under Article 10 or another means of co operation would be most appropriate. As a result, paragraph 6 provides that when a requested Party determines that it will not provide requested data to a Party that has made a request pursuant to paragraph 1 of this article, the requested Party shall inform the requesting Party of its determination on a rapidly expedited basis, and, if applicable, shall specify any conditions under which it would provide the data and explain any other forms of co-operation that may be available, in an effort to achieve the Parties' mutual goal of expediting disclosure of data in emergencies.

Paragraph 7

170. Paragraph 7 describes the applicable procedures where the requested State has specified conditions on the granting of co-operation under paragraph 6. Under paragraph 7.a, where the requesting Party is unable to comply with specified conditions, it must promptly bring this to the attention of the requested Party and the requested Party shall then make a determination as to whether the assistance may still be granted. By contrast, where the requesting Party has accepted a specified condition, it shall be bound by it. Under paragraph 7.b, a requested Party that has provided information or material subject to a condition under paragraph 6 may, in order to ascertain whether such condition has been complied with, require that the requesting Party explain the use it has made of the information or material provided, but it was understood that the requesting Party may not call for an overly burdensome accounting (see explanatory report, paragraphs 279 and 280, of the Convention).

Section 4 – Procedures pertaining to emergency mutual assistance

Article 10 – Emergency mutual assistance

171. Article 10 of this Protocol is intended to provide a rapidly expedited procedure for mutual assistance requests made in emergency situations. An emergency is defined in Article 3, paragraph 2.c, and explained in the related paragraphs 41 and 42 of this explanatory report.

172. Because Article 10 of this Protocol is limited to the emergencies justifying such rapidly expedited action, it is distinct from Article 25, paragraph 3, of the Convention, in which requests for mutual assistance may be made by expedited means of communications in urgent circumstances that do not rise to the level of emergency as defined. In other words, Article 25, paragraph 3,

is broader in scope than Article 10 of this Protocol, in that it covers situations not covered in Article 10, such as ongoing but non-imminent risks to life or safety of persons, potential destruction of evidence that may result from delay, a rapidly approaching trial date, or other types of urgencies. While the mechanism in Article 25, paragraph 3, provides for a more rapid method of conveying and responding to a request, the obligations in the case of an emergency under Article 10 of this Protocol are significantly greater; that is, where there is significant and imminent risk to life or safety of a natural person, the process should be even more accelerated (see paragraph 42 of this explanatory report for examples of emergency situations).

Paragraph 1

173. Under paragraph 1, in making an emergency request, the requesting Party must both conclude that an emergency within the meaning of Article 3, paragraph 2.c, exists and include in its request a description of the facts that demonstrate this, explaining the manner in which the assistance sought is necessary to respond to the emergency, in addition to the other information required to be contained in the request under the applicable treaty or domestic law of the requested Party. In this regard, it should be recalled that under Article 25, paragraph 4, of the Convention, execution of requests for mutual assistance generally "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 drafters understood this to apply also to emergency mutual assistance requests under this Protocol.

Paragraph 2

174. Paragraph 2 requires the requested Party to accept the mutual assistance request in electronic form. Before accepting the request, the requested Party may make the acceptance of the request conditional on compliance by the requesting Party with appropriate levels of security and authentication. With respect to the security requirement contained in this paragraph, the Parties may decide among themselves whether there is a need for special security protections (including encryption) that may be necessary in a particularly sensitive case.

Paragraph 3

175. Where the requested Party requires additional information to come to the conclusion that there is an emergency within the meaning of Article 3,

paragraph 2.c, and/or that the other requirements for mutual assistance have been met, it is required by paragraph 3 to seek the additional information on a rapidly expedited basis. Similarly, paragraph 3 requires the requesting Party to provide the supplemental information in the same rapidly expedited manner. Both Parties should therefore do their utmost to avoid loss of time that could inadvertently contribute to a tragic result.

Paragraph 4

176. Under paragraph 4, once the needed information has been provided to enable the request to be executed, the requested Party is required to respond to the request on the same rapidly expedited basis. This generally means rapidly expediting the obtaining of judicial orders compelling a provider to produce data that are evidence of the offence and the equally rapid service of the order on the provider. Delays occasioned by provider response times to such orders should not be attributed to the authorities of the requested Party, however.

Paragraph 5

177. Under paragraph 5, all Parties shall ensure that members of its central authority or other authorities responsible for responding to mutual assistance requests are available on a twenty-four hours a day, seven days a week basis, in case emergency mutual assistance requests need to be made outside regular business hours. It should be recalled that in this regard the 24/7 Network under Article 35 of the Convention is available for co-ordination with the authorities responsible for mutual assistance. The obligation in this paragraph does not require the central authority or other authorities responsible for responding to mutual assistance requests to be staffed and operational at all times. Rather, that authority should implement procedures to ensure that staff may be contacted in order to review emergency requests outside normal business hours. The T-CY will informally endeavour to maintain a directory of such authorities.

Paragraph 6

178. Paragraph 6 provides a basis for the central authorities or other authorities responsible for mutual assistance to mutually determine an alternative channel for transmission of the responsive information or evidence, be it the mode of transmission or the authorities between whom it is transmitted. Thus, rather than the responsive information or evidence being sent back through the central authority channel habitually used to transmit information or evidence provided in the execution of the requesting Party's request, they

may mutually determine to use a different channel to speed up transmission, maintain the integrity of the evidence or for another reason. For example, in an emergency, the authorities may decide on the transmission of evidence directly to an investigating or prosecuting authority in the requesting Party that will be using the evidence, rather than through the chain of authorities through which such evidence would normally travel. The authorities may also decide, for example, on special handling for physical evidence in order to be able to rule out challenges in subsequent judicial proceedings that the evidence may have been altered or contaminated, or may mutually decide on special handling of the transmission of sensitive evidence.

Paragraph 7

179. With respect to the procedures that govern this article, there are two possibilities, as described in paragraphs 7 and 8. Paragraph 7 of Article 10 provides that when the Parties concerned are not mutually bound by an applicable mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, the Parties apply certain procedures set forth in specified paragraphs of Articles 27 and 28 of the Convention (governing mutual assistance in the absence of a treaty).

Paragraph 8

180. Paragraph 8 provides that when the Parties concerned are mutually bound by such an agreement or arrangement, Article 10 is supplemented by the provisions of that agreement or arrangement unless the Parties concerned mutually determine to apply any or all of the provisions of the Convention referenced in paragraph 7, in lieu thereof.

Paragraph 9

181. Finally, paragraph 9 provides for a possibility for a declaration by which Parties to this Protocol can provide for requests to be made directly between prosecutors or other judicial authorities. In some Parties, such direct judicial authority to judicial authority channels are well established and may provide an efficient means of further accelerating the making of and execution of requests. The transmission of the emergency request through the Party's 24/7 point of contact or through the International Criminal Police Organization (INTERPOL) is useful not only to reduce any delay but also to increase standards of security and authentication. However, in some Parties, the sending of a request directly to a judicial authority in the requested Party without the involvement and approval of its central authority could be counter-productive in that, without

guidance and/or approval from its central authority, the receiving authority may not be empowered to act independently, or may not be familiar with the proper procedure. Therefore, a Party must declare that requests may be sent through these non-central authority channels.

Section 5 – Procedures pertaining to international co-operation in the absence of applicable international agreements

182. As provided in Article 5, paragraph 5, this section, relating to Articles 11 and 12, applies "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 section 5 shall not apply where such treaty or arrangement exists, except as provided in Article 12, paragraph 7. However, the Parties concerned may mutually determine to apply the provisions of section 5 in lieu thereof, if the treaty or arrangement does not prohibit it". This follows the approach of Article 27 of the Convention.

183. Between some Parties to this Protocol, the subjects of Articles 11 and 12 are already regulated through the terms of mutual assistance treaties (for example the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182) or the Agreement on mutual legal assistance between the European Union and the United States of America). Mutual assistance treaties such as ETS No. 182 may also provide more detail regarding the circumstances, conditions and procedures under which such co-operation may take place.

184. Although the drafters considered these treaties, Articles 11 and 12 of this Protocol contain terms that vary from analogous provisions in other mutual assistance treaties.

185. While the terms of ETS No. 182 will continue to be applied between the Parties to it, it was considered appropriate to regulate these two articles in this Protocol in a manner that differs in some respects for the following reasons:

– The membership of ETS No. 182 is different from that of the Convention on Cybercrime and its provisions are thus not available for co-operation between all the Parties to the Convention on Cybercrime. ETS No. 182 was negotiated to meet the needs of the member States of the Council of Europe rather than the legal requirements, systems and needs of all the Parties to the Convention on Cybercrime, although, in principle, the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30) and its

protocols are open for accession by non-member States of the Council of Europe following an invitation by the Committee of Ministers.

– The mutual assistance provisions of this Protocol have a specific material scope in that they apply to "specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence" (Article 2). Given the particular problems of this type of investigation or proceeding – such as the volatility of data, questions related to territoriality and jurisdiction, and to the volume of requests – the analogous provisions of ETS No. 182 may not always be applicable in the same way.

– The drafters recognised that "[a]s the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure" (see paragraph 145 of the explanatory report to the Convention). Instead, Parties are required to ensure that they provide "adequate protection of human rights and liberties" and apply "common standards [and] minimum safeguards to which Parties … must adhere", including "safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments" (see paragraph 145 of the explanatory report to the Convention). See Article 13 to this Protocol (incorporating Article 15 of the Convention). Therefore, in contrast to the provisions of ETS No. 182 – for example Article 9 on "hearing by video conference" – which prescribe specific procedures and safeguards to be followed by Parties to ETS No. 182, the corresponding provisions of this Protocol permit more flexibility in the Parties' implementation. For instance, the procedures and conditions governing the operation of joint investigation teams shall be as agreed between the Parties' competent authorities (see Article 12, paragraph 2), and with respect to video conferencing, a requested Party may require particular conditions and safeguards when permitting the hearing of a suspect or accused person via video conference (see Article 11, paragraph 8). To the extent provided in these articles, Parties may also decide not to co-operate if their requirements in terms of conditions and safeguards are not met.

186. Articles 11 and 12 of this Protocol apply only in the absence of other mutual assistance treaties or arrangements on the basis of uniform or reciprocal legislation – unless the Parties concerned mutually determine to apply any or all of their provisions in lieu thereof, if the treaty or arrangement does not prohibit it. However, Article 12, paragraph 7, applies whether or not there is a

mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned.

Article 11 – Video conferencing

187. Article 11 primarily addresses the use of video conferencing technology to take testimony or statements. This form of co-operation may be provided for in existing bilateral and multilateral mutual assistance treaties, for example ETS No. 182. In order to not supersede provisions specifically designed to meet the requirements of the Parties to those treaties or conventions, and as stated in the general principles applicable to this section (Article 5, paragraph 5), Article 11, like Article 12 in this Protocol, "applies 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 section 5 shall not apply where such treaty or arrangement exists, except as provided in Article 12, paragraph 7. However, the Parties concerned may mutually determine to apply the provisions of section 5 in lieu thereof, if the treaty or arrangement does not prohibit it".

Paragraph 1

188. Paragraph 1 authorises the taking of testimony and statements from a witness or expert by video conferencing. This paragraph gives the requested Party discretion whether or not to accept the mutual assistance request or to set conditions in providing assistance. For example, a Party may decline or postpone assistance on the grounds provided in Article 27, paragraphs 4 to 5, of the Convention. Alternatively, where it would be more effective for assistance to be rendered in a different manner, such as through a written form authenticating official or business records, the requested Party may opt to provide assistance in that manner.

189. At the same time, it is expected that Parties to this Protocol will have the basic technical capability to provide assistance via video conferencing.

190. Carrying out a video conference to take testimony or a statement can give rise to many issues, which may include legal, logistical and technical problems. In order that the video conference functions smoothly, advance co-ordination is essential. Additional co-ordination may be needed when the requested Party sets conditions as prerequisites to carrying out the video conference. Therefore, paragraph 1 also requires the requesting and requested Parties to consult where needed to facilitate the resolution of any such issues that arise. For example, as explained further below, the video conference may

need to follow a certain procedure in order for the result to be admissible as evidence in the requesting Party. Conversely, the requested Party may need to apply its own legal requirements in certain respects (for example the taking of an oath by, or advising of rights to, the witness). Moreover, the requested Party may require its official(s) to be present in the video conference in some or all situations, whether for the purpose of presiding over the procedure, or to ensure that the rights of the person whose testimony or statement is taken are respected. In this regard, the consultations may reveal that some requested Parties require that its participating official be able to intervene, interrupt or stop the hearing in case of concerns regarding conformity with its law, while other Parties may permit a video conference to take place without the participation of its officials in some circumstances. As a further example, requested Parties may seek particular safeguards with respect to witnesses whose safety is at risk, child witnesses, and similar. These matters are required to be discussed and decided upon in advance. In some cases, the requested Party's desire for one procedure may conflict with the laws of the requesting Party to facilitate use of the testimony or statement at trial. In such cases, the Parties should do their best to try to find creative solutions that meet the needs of both sides. In addition, the Parties shall consult in advance to facilitate resolution of issues, such as how to handle objections or claims of privilege or immunity raised by the person or their legal counsel, or the use of documentary or other evidence, during the video conference. Also, particular procedures may be required because of conditions imposed in order for a video conference to take place.

Logistical questions, such as whether the requesting Party should provide for interpretation and recording of the testimony or statement from its side of the video conference or the requested Party from its side, should also be discussed, as well as technical co-ordination to initiate and maintain the transmission and have alternative channels of communication in the event that the transmission is interrupted.

Paragraph 2

191. Paragraph 2 addresses a number of procedural and related mechanisms governing this form of co-operation (in addition to other applicable procedures and requirements set out in the remaining paragraphs of this article), which have been taken or adapted from the Convention. Paragraph 2 is divided into two sub-paragraphs.

192. Since video conferencing is a form of mutual assistance, paragraph 2.a provides that the central authorities of the requested and requesting Parties

shall communicate directly with each other for the purposes of applying this article. Because this article only applies in the absence of a mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, "central authority" here means the authority or authorities designated under Article 27, paragraph 2.a, of the Convention (see Article 3, paragraph 2.a, of this Protocol and paragraph 38 of the explanatory report).

193. Paragraph 2.a of this article also provides that a requested Party may accept a request for video conferencing in electronic form, and it may require appropriate levels of security and authentication before accepting the request.

194. Paragraph 2.b requires (similar to Article 27, paragraph 7, of the Convention) the requested Party to inform the requesting Party of its reasons for not executing a request or for delaying the execution of the request. As stated in paragraph 192 above, such communications shall take place via central authority channels. Finally, paragraph 2.b provides that Article 27, paragraph 8 (addressing confidentiality of a mutual assistance request in the absence of a treaty), and Article 28, paragraphs 2 to 4 (addressing confidentiality of the response and use limitations in the absence of a treaty), of the Convention apply to the video conferencing article.

Paragraph 3

195. Since a video conference may require judicial and auxiliary officials in a requesting Party to be available to participate in the taking of testimony or statement in the requested Party, many time zones away, it is critical that the person to be heard appears at the scheduled time and place. Under paragraph 3, where the requested Party provides assistance under this article, it must endeavour to obtain the presence of the person whose testimony or statement is sought. How to best do so may depend on the circumstances of the case, domestic law of the requested Party and whether, for example, there is confidence that the person will appear at the scheduled time voluntarily. In contrast, in order to ensure that the person appears, it may be advisable for the requested Party to issue an order or summons compelling the person to appear, and this paragraph authorises it to do so, in accordance with the safeguards set forth in its domestic law.

Paragraph 4

196. The procedure relating to the conduct of video conferences is set forth in paragraph 4. The key objective is to provide the testimony or statement to the requesting Party in a form that will permit its use as evidence in its

investigation and proceedings. For that reason, the procedures requested by the requesting Party shall be applied, unless to do so would be incompatible with the law of the requested Party, including the requested Party's applicable legal principles not codified in its legislation. For example, during the video conference, the preferred procedure would be for the requested Party to permit the authorities of the requesting Party to directly question the person from whom testimony or statements are sought. It will be the requesting Party's prosecutor, investigating judge or investigator that knows the criminal investigation or prosecution most deeply, and therefore knows best which questions are most useful for the investigation or prosecution, as well as how best to phrase them in the way to comply with the requesting Party's law. In that case, the authority of the requested Party participating in the hearing would intervene only if necessary because the requesting Party authority proceeded in a way incompatible with the requested Party's law. In that case, the requested Party may disallow questions, take over questioning or take other action as may be appropriate under its law and the circumstances of the video conference. The term "incompatible with the law of the requested Party" does not encompass situations in which the procedure is merely different from that in the requested Party, which will often be the case. Rather, it is intended to address situations in which the procedure is contrary to or unworkable under the requested Party's law. In such cases, or where no specific procedure is sought by the requesting Party, the default procedure will be the procedure applicable under the requested Party's law. If application of the requested Party's law causes a problem for the requesting Party, for example in terms of the admissibility of the testimony or statement at trial, the requesting and requested Parties can seek to reach agreement on a different procedure that will satisfy the requesting Party yet avoid the problem under the law of the requested Party.

Paragraph 5

197. The purpose of paragraph 5, concerning penalty or sanction for false statement, refusal to answer and other misconduct, is to protect the integrity of the process of providing testimony or statement when the witness is physically in a different country than that in which the criminal proceeding is taking place. To the extent that the requested Party has placed the person under an obligation to testify or to testify truthfully, or has prohibited the person from engaging in certain conduct (for example disrupting the proceedings), the witness will become subject to consequences in the jurisdiction where the witness is located. In such cases, the requested Party must be able to apply

the sanction it would apply if such conduct took place in the course of its own domestic proceedings. It shall apply without prejudice to any jurisdiction of the requesting Party. This requirement provides a further incentive for the witness to testify, testify truthfully and not engage in prohibited conduct. If there is no sanction that would apply in the requested Party's domestic proceedings (for example for a false statement by an accused person), it is not required to establish any for such conduct committed during a video conference. This provision will be particularly useful to ensure the prosecution of a witness who testifies falsely but cannot be extradited to face prosecution in the requesting Party because, for example, of a requested Party's prohibition on extradition of nationals.

Paragraph 6

198. Paragraph 6 provides rules regarding the allocation of costs arising in the course of video conferences. As a general rule, all costs arising in the course of a video conference are borne by the requested Party, except for (i) fees of an expert witness; (ii) costs of translation, interpretation and transcription; and (iii) costs that are so significant as to be of an extraordinary nature. Travel costs and costs for overnight stays within the requested Party most often are not substantial, so that such costs, if any, generally are absorbed by the requested Party. The rules regarding costs may be modified by the agreement between the requesting and requested Parties, however. For example, if the requesting Party provides for the presence of an interpreter who is needed or for transcription services at its end of the video conference, there may well be no need for it to pay for the requested Party to furnish such services. When the requested Party foresees extraordinary costs in providing assistance, in accordance with paragraph 6.b, the requesting Party and the requested Party shall consult prior to execution of the request in order to determine if the requesting Party can bear these costs and, if not, how they can be avoided.

Paragraph 7

199. While paragraph 1 expressly authorises the use of video conferencing technology for taking testimony or statement, paragraph 7.a provides that the provisions of Article 11 may be applied for the purposes of carrying out audio conferences where so mutually agreed. In addition, paragraph 7.b provides that, where agreed upon by the requesting and requested Parties, the technology may be used for other "purposes, or for hearings, … including for the purposes of identifying persons or objects". Thus, if mutually agreed, the requesting and requested Parties may contemplate using video conferencing

technology in order to hear or carry out proceedings regarding a suspect or accused (it should be noted that some Parties may consider a suspect or accused to be a "witness" so that the taking of that person's testimony or statement would already be covered by paragraph 1 of this article). Where paragraph 1 is not applicable, paragraph 7 provides legal authority to permit the use of the technology in such instances.

Paragraph 8

200. Paragraph 8 addresses the situation in which the requested Party chooses to permit the hearing of a suspect or accused person, such as for the purposes of giving testimony or statements, or for notifications or other procedural measures. In the same manner as the requested Party has discretion to permit a video conference of an ordinary witness or expert, it has discretion with respect to a suspect or accused person. Furthermore, in addition to any other condition or limitation a requested Party may impose in order to permit the carrying out of a video conference, a Party's domestic law may require particular conditions with respect to the hearing of suspects or accused persons. For example, a Party's law may require consent of the suspect or accused person to provide testimony or statement, or a Party's law may prohibit or limit the use of video conference for notifications or other procedural measures. Thus, paragraph 8 is intended to give emphasis to the fact that procedures aimed at a suspect or accused person may give rise to the need for conditions or safeguards supplemental to those that might otherwise arise.

Article 12 – Joint investigation teams and joint investigations

201. Given the transnational nature of cybercrime and electronic evidence, investigations and prosecutions related to cybercrime and electronic evidence often have links to other States. Joint investigation teams (JITs) can be an effective means for operational co-operation or co-ordination between two or more States. Article 12 provides a basis for such forms of co-operation.

202. Experience has shown that where a State is investigating an offence with a cross-border dimension in relation to cybercrime or for which electronic evidence needs to be obtained, the investigation can benefit from the participation of the authorities of other States that are also investigating the same or related conduct or where co-ordination is otherwise useful.

203. As indicated in Article 5 of this Protocol and explanatory report paragraphs 182 to 186, the provisions of Article 12 shall not apply where there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal

legislation in force between the requesting and requested Parties, unless the Parties concerned mutually determine to apply any or all of the remainder of this article in lieu thereof, if the treaty or arrangement does not prohibit it. As explained below, paragraph 7 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned.

Paragraph 1

204. Paragraph 1 states that the competent authorities of two or more Parties may agree to set up a JIT where they deem it to be of particular utility. A JIT is entered into by mutual agreement. The terms "mutual agreement", "agreement" and "agree" – as used in Article 12 – should not be understood to require a binding agreement under international law.

205. This article uses two related terms: "competent authorities" and "participating authorities". Each Party determines which authorities are competent – that is, the "competent authorities" – to enter into a JIT agreement. Some Parties may authorise a range of officials, such as prosecutors, investigating judges or other senior law-enforcement officers directing criminal investigations or proceedings, to enter into such an agreement; others may require the central authority – the office normally responsible for mutual assistance matters – to do so. The decision as to which authorities actually participate in a JIT – the "participating authorities" – similarly will be determined by the respective Parties.

Paragraph 2

206. Paragraph 2 provides that the procedures and conditions under which the joint investigation teams are to operate, such as their specific purposes; composition; functions; duration and any extension periods; location; organisation; terms of gathering, transmitting and using information or evidence; terms of confidentiality; and terms for the involvement of the participating authorities of a Party in investigative activities taking place in another Party's territory, shall be as agreed between those competent authorities. In particular, when preparing the agreement, the Parties concerned may wish to discuss the terms for refusing or restricting use of information or evidence, including, for example, on the grounds established in Article 27, paragraphs 4 or 5, of the Convention, and what procedure to follow if the information or evidence is needed for purposes other than those for which the agreement has been entered into (including use of the information or evidence by the prosecution

or defence in another case or where it may be needed to prevent an emergency as defined in Article 3, paragraph 2.c, that is, a situation in which there is a significant and imminent risk to the life or safety of a natural person). Parties are encouraged to specify in the agreement the limits on the powers of participating officials of a Party who are physically present in the territory of another Party. The Parties are also encouraged to permit in the agreement the electronic transmission of the information or evidence gathered.

207. It is anticipated that Parties will generally mutually determine these procedures and conditions in writing. In any agreement, consideration should be given to the level of detail required. A streamlined text may provide the necessary level of precision for foreseeable circumstances, with the ability to add supplementary provisions should future circumstances require further precision. The Parties shall consider the geographic scope and duration of the JIT agreement and the fact that the agreement may need to be modified or enlarged as new facts become available.

208. The information or evidence used as part of the joint investigation team may include personal data in the form of subscriber information, traffic data or content data. As in the case of other co-operative measures under this Protocol, Article 14 applies to the transfer of personal data pursuant to JITs.

209. As generally is the case with respect to all information or evidence received by a Party pursuant to this Protocol, that Party's applicable rules of evidence will govern whether the information or evidence will be admissible in judicial proceedings.

Paragraph 3

210. Paragraph 3 permits a Party to declare at the time of signature of this Protocol, or when depositing its instrument of ratification, acceptance or approval, that its central authority must be a signatory to, or otherwise concur in the agreement establishing the team. This provision was inserted for several reasons. First, a number of Parties consider JITs to be a form of mutual assistance, and in a number of other Parties, central authorities for mutual assistance may play a role in ensuring that applicable domestic legal requirements are met when competent authorities (which may be prosecutors or police with relatively limited international co-operation experience) are preparing a JIT agreement under this article. A central authority's experience with international agreements governing mutual assistance and other forms of international co-operation (including this Protocol) can also help it to play a valuable role in ensuring that the Protocol's requirements are met.

Finally, if a Party has made the declaration provided for under this paragraph, the authorities of other Parties seeking to enter into a JIT with the declaring Party are on notice that the declaring Party's central authority must sign or otherwise concur in the JIT agreement for it to be valid under the Protocol. This protects against the conclusion of a JIT agreement that does not have required authorisation or does not comply with applicable legal requirements of the declaring Party.

Paragraph 4

211. Under paragraph 4, the competent authorities determined by the Parties under paragraph 1 and the participating authorities described in paragraph 2 will normally communicate directly with each other to ensure efficiency and effectiveness. However, where exceptional circumstances may require more central co-ordination – such as cases with particularly serious ramifications or situations raising particular problems of co-ordination – other appropriate channels may be agreed. For example, the central authorities for mutual assistance may be available to assist in co-ordinating such matters.

Paragraph 5

212. Paragraph 5 foresees that where investigative measures need to be taken in the territory of one of the participating Parties, participating authorities of that Party may issue a request to their own authorities to carry out such measures. Those authorities determine whether they can take the investigative measure on the basis of their domestic law. Where they can do so, a request for mutual assistance by other participating Parties may not be required. This provides for one of the most innovative aspects of JITs. However, in some situations, those authorities may not have sufficient domestic authority to take a particular investigative measure on behalf of another Party without a request for mutual assistance.

Paragraph 6

213. Paragraph 6 addresses the use of information or evidence obtained by the participating authorities of one Party from the participating authorities of another Party. Use may be refused or restricted in accordance with the terms of an agreement described in paragraphs 1 and 2; however, if that agreement does not provide terms for refusing or restricting use, the information or evidence may be used in the manner provided in paragraphs 6.a to c. The circumstances set out in paragraph 6 are without prejudice to the requirements set out for onward transfers of information or evidence to another State in Article 14.

14. It should be noted, that when paragraphs 6.a to c apply, the participating authorities may nonetheless mutually decide to further limit use of particular information or evidence in order to avoid adverse consequences to one of their investigations, either before, or particularly after, the information or evidence has been provided. For example, even if the use of evidence is for a purpose for which the JIT was established by the Party that has received it, it may have an adverse impact on the investigation of the Party providing the information or evidence (such as by revealing the existence of the investigation to a criminal group, thus potentially causing criminals to flee, destroy evidence or intimidate witnesses). In that case, the Party that provided the information or evidence may ask the other Party to consent to not make it public until this risk is no longer present.

215. In paragraph 6.b, the drafters intended that, in the absence of an agreement providing terms for refusing or restricting use, consent of the authorities providing the information or evidence would not be required where, under the fundamental legal principles of the Party whose participating authorities received it, information or evidence important to conducting an effective defence in the proceedings relating to those other offences must be disclosed to the defence or a judicial authority. Even though in this case consent is not required, notification of the disclosure of the information or evidence for this purpose shall be provided without undue delay. If possible, such notification should be provided in advance of disclosure, to enable the Party that provided the information or evidence to prepare for the disclosure and permit the Parties to consult as appropriate.

216. The drafters understood that paragraph 6.c refers to exceptional circumstances where the receiving Party's authorities could directly use the information or evidence to prevent an emergency as defined in Article 3, paragraph 2.c, of this Protocol. Safety of a natural person means serious bodily harm. The concept of a "significant and imminent risk to the life or safety of any natural person" is explained in more detail in paragraph 42 of the explanatory report, which also provides examples of such situations. The drafters considered that cases where a significant and imminent threat to assets or networks involves the life or safety of a natural person would be included in such a concept. In cases where information or evidence is used under paragraph 6.c, the participating authorities of the Party that provided the information or evidence shall be notified without undue delay of such use, unless mutually determined otherwise. For instance, the participating authorities may determine that the central authority should be notified.

Paragraph 7

217. Lastly, it should be generally recalled that there is a long history of international co-operative efforts carried out between law-enforcement partners on an ad hoc basis in which a team of prosecutors and/or investigators from one country has co-operated with foreign counterparts in a particular investigation, other than on the basis of a JIT. Paragraph 7 provides for these international co-operative efforts and provides a treaty basis for entering into a joint investigation in the absence of an agreement described in paragraphs 1 and 2, should a Party require such a legal basis. This paragraph applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned. As with all measures under this Protocol, joint investigations under paragraph 7 are subject to the conditions and safeguards of Chapter III.

Chapter III – Conditions and safeguards

Article 13 – Conditions and safeguards

218. Based on Article 15 of the Convention, Article 13 provides that "each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties". As this article is based on Article 15 of the Convention, the explanation of that article in paragraphs 145 to 148 of the explanatory report to the Convention is also valid for Article 13 of this Protocol, including that the principle of proportionality "shall be implemented by each Party in accordance with relevant principles of its domestic law" (see paragraph 146 of the explanatory report to the Convention).

219. It should be noted that in addition to this article, other articles contain important safeguards. For example, the measures of this Protocol are limited in scope, that is, "to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence" (see Article 2). In addition, individual articles specify information to include in requests, orders and accompanying information that may assist in applying domestic safeguards (see Article 6, paragraph 3; Article 7, paragraphs 3 and 4; Article 8, paragraph 3; Article 9, paragraph 3). Additionally, the types of data to be disclosed are specified in each article, such as, for example, in Article 7 which is limited to subscriber information. Also, Parties may make reservations and

declarations, for example to limit the type of information to be provided, such as in Articles 7 and 8. Finally, where personal data are transferred pursuant to this Protocol, the data protection safeguards of Article 14 apply.

Article 14 – Protection of personal data

Paragraph 1 – Scope

220. The measures provided for in Chapter II of this Protocol often involve the transfer of personal data. Given that many Parties to this Protocol may be required, in order to meet their constitutional or international obligations, to ensure the protection of personal data, Article 14 provides for data protection safeguards to permit Parties to meet these requirements, and thus to enable the processing of personal data for the purposes of this Protocol.

221. Pursuant to paragraph 1.a, each Party shall process personal data that it receives under this Protocol in accordance with the specific safeguards set out in paragraphs 2 to 15. This includes personal data transferred as part of an order or request under this Protocol. However, paragraphs 2 to 15 do not apply if the terms of the exceptions articulated in paragraphs 1.b or 1.c are applicable.

222. The first exception is set forth in paragraph 1.b, which provides that "[i]f at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under the Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned". In this context, a framework would generally be considered as being "comprehensive" where it comprehensively covers the data protection aspects of the data transfers. Two examples of agreements under paragraph 1.b are the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by Protocol CETS No. 223, and the Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection,

and Prosecution of Criminal Offenses. The terms of such agreements shall apply in lieu of paragraphs 2 to 15 for the measures falling within the scope of such agreements. With respect to the Parties to Convention ETS No. 108 as amended by Protocol CETS No. 223, this means that Article 14, paragraph 1, of that treaty, as further explained in paragraphs 105 to 107 of its explanatory report, is applicable. In terms of timing, paragraphs 2 to 15 of this article will be superseded only if the Parties are mutually bound by the agreement at the time of receipt of personal data under this Protocol. This applies for as long as the agreement provides that data transferred pursuant to it continues to be processed under the terms of that agreement.

223. The second exception is set forth in paragraph 1.c which provides that, even if the transferring Party and the receiving Party are not mutually bound under an agreement of the kind described in paragraph 1.b, they may nevertheless mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between them in lieu of paragraphs 2 to 15 of this article. This ensures that Parties retain flexibility in determining the data protection safeguards that apply to transfers between them under the Protocol. In order to provide for legal certainty and transparency for individuals and for the providers and entities involved in data transfers pursuant to measures in Chapter 2, section 2, of this Protocol, the Parties are encouraged to clearly communicate to the public their mutual determination that such an agreement or arrangement governs the data protection aspects of personal data transfers between them.

224. The drafters considered that, through the data protection safeguards set forth in paragraphs 2 to 15 of this article, this Protocol ensures appropriate protections for data transfers under this Protocol. To that end, pursuant to paragraph 1.d, data transfers under paragraph 1.a shall be deemed to meet the requirements of the data protection legal framework for international transfers of personal data of each Party, and no further authorisation for such transfers shall be required under such legal frameworks.

Additionally, insofar as the agreements described in paragraph 1.b provide by their terms that the processing of personal data under those agreements complies with the requirements of the data protection legislation of the Parties concerned, paragraph 1.d extends this endorsement to transfers under this Protocol. This paragraph thus provides legal certainty for international transfers of personal data in accordance with paragraphs 1.a or 1.b in response to orders and requests under this Protocol in order to ensure the effective and predictable exchange of data. Because agreements or arrangements described

in paragraph 1.c may not always reference compliance with the Parties' data protection legal framework for international transfers – for example in the case of bilateral mutual assistance treaties – they do not receive the same endorsement under this Protocol as for paragraphs 1.a or 1.b. However, the Parties concerned may provide for such an endorsement by mutual determination.

225. In addition, paragraph 1.d provides that a Party may only refuse or prevent personal data transfers to another Party under this Protocol for reasons of data protection: (i) under the conditions set out in paragraph 15 regarding consultation and suspension, when paragraph 1.a applies, or (ii) under the terms of the specific agreements or arrangements referred to in paragraphs 1.b or 1.c, when one of those paragraphs applies.

226. Finally, the objective of Article 14 is to establish appropriate safeguards permitting the transfer of personal data between Parties under this Protocol. Article 14 does not require the harmonisation of domestic legal frameworks for the processing of personal data generally, nor of the framework for the processing of personal data for the purposes of criminal law enforcement specifically. Paragraph 1.e provides that Parties are not precluded from applying stronger data protection safeguards than those provided in paragraphs 2 to 15 to the processing, by their own authorities, of personal data that those authorities receive under this Protocol. Conversely, paragraph 1.e. is not intended to permit Parties to impose additional data protection requirements for data transfers under this Protocol beyond those specifically allowed in this article.

Paragraph 2 – Purpose and use

227. Paragraph 2 addresses the purposes and use for which Parties may process personal data under this Protocol. Paragraph 2.a provides that "the Party that has received personal data shall process them for the purposes described in Article 2", that is, for the purpose of "specific criminal investigations or proceedings concerning criminal offences related to computer systems and data" and for the "collection of evidence in electronic form of a criminal offence", and as between Parties to the First Protocol, for the purpose of "specific criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol". In other words, authorities must be investigating or prosecuting specific criminal activity, which is the legitimate purpose for which evidence or information containing personal data may be sought and processed.

228. While, in the first instance, this Protocol may only be invoked in order to obtain information or evidence in a specific criminal investigation or proceeding

rather than for other purposes, paragraph 2.a also provides that a Party "shall not further process the personal data for an incompatible purpose, and it shall not further process the data when this is not permitted under its domestic legal framework". In determining whether the purpose of further processing is not incompatible with the initial purpose, the competent authority is encouraged to make an overall assessment of the specific circumstances, such as (i) the relationship between the initial and further purpose (for example any objective link); (ii) the (potential) consequences of the intended further use for the individuals concerned, taking into account the nature of the personal data (for example their sensitivity); (iii) any reasonable expectations of the individuals concerned regarding the purpose of further use and which entities might process the data; and (iv) the manner in which the data will be processed and protected against improper use. The legal framework of a Party may further set out particular limitations regarding other purposes for which the data may be used.

229. Processing for a not incompatible purpose would ordinarily include use of the data for international co-operation pursuant to domestic laws and international agreements or arrangements (for example mutual assistance) in the area of criminal law. It could also include, among other things, uses for certain governmental functions, such as reporting to oversight bodies; related inquiries into violations of criminal, civil or administrative law (including inquiries by other government components) and their adjudication; disclosures required by domestic court orders; disclosure to private litigants; disclosing certain information to the counsel for an accused; and disclosing directly to the public or news media (including in the context of access to document requests and public legal proceedings). Equally, the further processing of personal data for the purposes of archiving in the public interest, scientific or historical research or statistical purposes could be considered as compatible.

230. Paragraph 2.a further permits Parties to impose additional conditions and limitations on the use of personal data in individual cases, to the extent provided in Chapter II of this Protocol. However, such conditions shall not include generic data protection conditions – that is, those that are not case-specific – beyond those provided by Article 14. As an example, different systems for oversight are accepted under paragraph 14 and a Party may not make it a condition of transfer in an individual case that the requesting Party has the equivalent of a specialised data protection authority.

231. Finally, paragraph 2.b requires that in seeking and using personal data pursuant to this Protocol, "[t]he receiving Party shall ensure under its domestic

legal framework that personal data sought and processed are relevant to and not excessive in relation to the purposes of such processing". This requirement may be implemented via, for example, rules of evidence and limitations on the breadth of compulsory orders, the principles of necessity and proportionality, principles of reasonableness, and internal guidelines and policies that limit data collection or use. Parties are also encouraged to consider, under their domestic legal frameworks, situations involving vulnerable individuals, such as, for instance, victims or minors.

Paragraph 3 – Quality and integrity

232. Paragraph 3 requires Parties to "take reasonable steps to ensure that personal data are maintained with such accuracy and completeness and are as up to date as is necessary and appropriate for the lawful processing of the personal data, having regard to the purposes for which they are processed". The context is important, so that this principle may be implemented differently according to the circumstances. For example, the principle would be applied differently for criminal proceedings than for other purposes.

233. Regarding criminal investigations and proceedings, paragraph 3 should not be viewed as requiring criminal law-enforcement authorities to alter information – even if such information is inaccurate or incomplete – that may constitute evidence in a criminal case, as the data's inaccuracy may be central to the crime (for example in fraud cases), and it would also undermine the goal of fairness to the accused were authorities to modify a piece of evidence that was gathered via this Protocol.

234. In many situations, when there are doubts about the reliability of the personal data, this should be clearly indicated. For example, to the extent information or evidence that has been received via this Protocol is used to track past criminal conduct, applicable procedures should provide means for correcting or memorialising errors in the information (such as by amending or supplementing the original information), and for updating, amending or supplementing unreliable or out-of-date data, in order to minimise the risk that authorities would take inappropriate and potentially adverse law-enforcement actions on the basis of poor data quality (for example, arresting the wrong person or arresting a person in reliance on an incorrect understanding of his or her conduct). Parties are encouraged to take reasonable steps to ensure that where data provided to or received from another authority are found to be incorrect or outdated, the other authority is informed as soon as practicable

in order to make corrections to the extent necessary and appropriate given the purposes of processing.

Paragraph 4 – Sensitive data

235. Paragraph 4 concerns the measures to be taken under this Protocol by Parties when handling certain types of data that may be needed, in particular, as evidence in a criminal investigation or proceeding, but at the same time are of such a nature that appropriate safeguards are needed to guard against the risk of unwarranted prejudicial impact to the individual concerned from the use of such data, in particular against unlawful discrimination.

236. Paragraph 4 provides that sensitive data include "personal data revealing racial or ethnic origin; political opinions, religious or other beliefs, or trade union membership; genetic data; biometric data considered sensitive in view of the risks involved; or personal data concerning health or sexual life", which would include both sexual orientation and sexual practices. Health data may include data related to a person's physical or mental health that reveals information about his or her past, present or future health status (for example, information about a disease, disability, disease risk, a person's medical history or treatment, or the physiological or biomedical state of the person). Genetic data may include, for example, data that result from chromosomal, DNA or RNA analysis and relate to the inherited or acquired genetic characteristics of a person that contain unique information about his or her physiology, health or filiation.

237. The concept of biometric data covers a range of unique identifiers resulting from measurable physical or physiological characteristics used to identify, or verify the claimed identity of, an individual (for example fingerprints, iris or palm vein patterns, voice patterns, photographs or video-footage). Some Parties also consider unique identifiers resulting from biological or behavioural characteristics to constitute biometric data. While certain forms of biometric data may be considered sensitive in view of the risks involved, other forms may not. For example, some Parties consider biometric data that are computed or extracted from a biometric sample or image (such as biometric templates) as sensitive. Conversely, certain photographs or video-footage, even if they reveal physical or anatomical features such as scars, skin marks and tattoos, would not generally be considered to fall into the category of sensitive biometric data. Because the level of sensitivity of biometric data may vary, paragraph 4 provides flexibility to Parties to regulate this area by indicating that sensitive data include "biometric data considered sensitive in view of the

risks involved". This language recognises that biometrics is an evolving field and what data are considered "sensitive" under this paragraph will need to be evaluated over time in conjunction with technological, investigatory and other developments and the risks to the individual involved. With respect to the Parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by Protocol CETS No. 223, the interpretation of what constitutes "sensitive" biometric data should be guided by Article 6, paragraph 1, of that treaty, as further detailed in paragraphs 58 and 59 of its explanatory report.

238. The misuse and improper processing of sensitive data presents potential risks of unwarranted prejudice to individuals, including risks of unlawful discrimination. The criminal justice system should be configured to guard against unwarranted prejudicial impact and unlawful discrimination based on, for example, the use of evidence revealing race, religion or sexual life. As another example, this paragraph also recognises the importance of guarding against the risk of harm caused by unwarranted or unlawful disclosure, for instance a person being ostracised based on information revealing sexual orientation or gender identity. In this regard, paragraph 4 requires Parties to provide for "appropriate safeguards" in order to guard against such risks.

239. The appropriateness of safeguards should be assessed by reference to the sensitivity of the data and the scope, context, purposes and nature of processing (for instance in the case of automated decision making), as well as the likelihood and severity of the risks. These safeguards may vary between domestic legal systems and depend on these factors. A non-exhaustive list of safeguards may include restricting the processing (for example allowing the processing only for certain purposes or on a case-by-case basis), limiting dissemination, restricting access (for example, limiting access only to certain personnel through special authorisation or authentication procedures, requiring specialised training for such personnel), additional organisational or technical security measures (for example, masking, pseudonymisation or separating storage of biometric data from the connected biographical information) or shorter retention periods. In certain cases, it may be useful to conduct an impact assessment to help identify and manage risks.

Paragraph 5 – Retention periods

240. The first sentence of paragraph 5 provides that "[e]ach Party shall retain the personal data only for as long as necessary and appropriate in view of the purposes of processing the data pursuant to paragraph 2". In this regard,

the purpose limitation principle of paragraph 2 provides that a Party that has received personal data shall process it for specific purposes in accordance with Article 2 and shall not further process it for an incompatible purpose. In line with that principle, the period for retention of data links to the specific purpose(s) for which the data are processed.

241. Because under Article 2, personal data received by a Party pursuant to this Protocol is for the purpose of specific criminal investigations or proceedings, the personal data may be kept as long as needed (i) for the duration of the investigation and subsequent proceeding, including any appeals or periods during which a case may be re-opened under domestic law; and (ii) after the purpose of the original collection has been fulfilled, for further processing for a purpose that is "not incompatible" with the original purpose. For instance, a Party may provide that information or evidence be kept for archiving or historical research purposes, or other compatible purposes in line with Article 14, paragraph 2, as further explained in the corresponding paragraphs of this explanatory report.

242. The second sentence of paragraph 5 gives the Parties two options to meet the obligation to retain personal data only for as long as necessary and appropriate in view of the purposes of processing the data pursuant to paragraph 2 of this article. First, a Party may provide for specified retention periods in its domestic legal framework. Alternatively, Parties may provide in their domestic legal framework for the review of the need for further retention at planned intervals. Parties have a margin of discretion to decide which approach, in the context of their domestic legal framework, best suits the specific set of data. Parties may also combine a specific retention period with a system of periodic review at shorter intervals. They should ensure in their legal framework that competent authorities develop internal rules and/or procedures for implementing the specific retention periods and/or periodic review of the need for further retention. If the retention period has expired or if the Party has determined through periodic review that there is no further need to retain the data, they should be deleted or rendered anonymous.

Paragraph 6 – Automated decisions

243. Paragraph 6 concerns the protection of individuals when decisions producing a significant adverse effect concerning their relevant interests are based solely on automated processing of their personal data. It is not anticipated that, when a Party receives personal data from another Party under this Protocol, automated decision making will often be involved because the evidence or information will be gathered by investigators or judicial authorities

for purposes of a specific criminal investigation or proceeding. Nevertheless, if automated decision making, producing a significant adverse effect concerning the relevant interests of the individual to whom the personal data relate, takes place in the investigation for which the data were sought, authorities must follow this provision. Authorities must also follow this provision if subsequent uses of the data take place for the prevention, detection, investigation or prosecution of other crimes (for example arrest based on purely automated processing of criminal profiles, sentencing, bail, parole), or for a compatible purpose (for example within the context of background checks), if the data are subject to automated analytical tools for decision-making purposes.

244. Paragraph 6, therefore, prohibits a decision based only on the automated processing of personal data where it produces a significant adverse effect concerning an individual's relevant interests, including adverse legal effects (by affecting the individual's legal status or rights), such as issuing an arrest warrant or denying bail or parole, unless such decision making is authorised under domestic law and subject to appropriate safeguards.

245. Appropriate safeguards are critical to reducing the potential impact to the relevant interests of the individual to whom the personal data relate. Such safeguards should cover the possibility for the individual concerned to obtain human intervention to assess the decision. Parties are also encouraged to take reasonable steps to provide for the quality and representativeness of the data used to develop algorithms and the accuracy of the statistical inferences used, taking into account the specific circumstances and context of processing, including the context of criminal law enforcement.

Paragraph 7 – Data security and security incidents

246. Pursuant to paragraph 7.a, "[e]ach Party shall ensure that it has in place appropriate technological, physical and organisational measures for the protection of personal data". For example, technological measures may include software protecting against computer malware, encryption of data and firewalls. Physical measures may include storage of computer servers and files in secure locations and organisational measures may include rules, practices, policies and procedures, including those that limit access rights.

247. Paragraph 7.a further provides that the measures must guard, in particular, against loss (for example standardised procedures for filing and handling data), accidental or unauthorised access (for example protections against computer intrusions, authorisation or authentication requirements for accessing paper or computer files), accidental or unauthorised disclosure (for example

technological measures to detect and prevent accidental or unauthorised disclosures, and organisational measures to outline consequences for such disclosures), and accidental or otherwise unauthorised alteration or destruction of data (for example restricting input or alteration of electronic data or paper files to authorised personnel, use of logging systems, display of retention periods, installation of computer or paper file backup systems).

248. The precise way of meeting these requirements, in a manner appropriate to the specific circumstances, is left to the Party concerned. Parties are encouraged, for example, to design and implement security measures that take into account such factors as the nature of the personal data (including its sensitivity), the identified risks and any potential adverse consequences for the individual concerned in case of a security incident. At the same time, Parties may take into account questions of the resources involved in designing and implementing data security measures. Parties are encouraged to subject such measures to periodic review and update them where appropriate in view of the development of technology and the evolving nature of the risks.

249. Paragraph 7.b sets out the requirements in the event of a "security incident" (as defined in paragraph 7.a and described above) with respect to personal data received under this Protocol that creates a "significant risk of physical or non-physical harm" to individuals or to the Party from which the data originated. Relevant harm to an individual may include for instance bodily or reputational harm, emotional distress (for example through humiliation or a breach of confidentiality), discrimination or financial harm (for example loss of employment or professional opportunities, negative credit rating, identity theft or potential for blackmail). As regards the other Party, relevant harm may in particular include the potential negative impact on a parallel investigation (for example absconding of the suspect, destruction of evidence). If there is a "significant risk" of such harm, the receiving Party has an obligation to "promptly assess the likelihood and scale" of the harm and to "promptly take appropriate action to mitigate such harm". Factors related to the likelihood and scale of harm to be considered may include, *inter alia,* the type of incident, such as, if known, whether it was malicious; the persons who have or could obtain the information; the nature and sensitivity of the affected data; the volume of data potentially compromised and the number of individuals potentially affected; the ease of identification of the individual(s) concerned; the likelihood of access and use of the data, for example whether the data were encrypted or otherwise rendered inaccessible; and possible consequences which may occur as a result of the incident.

250. In accordance with the measures described under paragraph 7.a and to ensure an appropriate response under paragraph 7.b, Parties are required to have internal processes in place to be able to discover security incidents. They should also have a process for promptly evaluating the likelihood and scale of the potential harm, and for promptly taking appropriate measures to mitigate harm (for example by recalling or requesting deletion of information that has accidentally been transmitted to an unauthorised recipient). The effective application of these requirements may benefit from internal reporting procedures and from keeping records of any security incident.

251. Paragraph 7.b also sets forth the circumstances in which the other Party and affected individual(s) must be notified regarding the incident, subject to exceptions and limitations.

252. In the event of a security incident in which there is a significant risk of physical or non-physical harm to individuals or to the other Party, notification shall be provided to the transferring authority or, for the purposes of Chapter II, section 2, to the authority or authorities designated pursuant to paragraph 7.c. However, notification may include appropriate restrictions as to the further transmission of the notification, be delayed or omitted when such notification may endanger national security or be delayed when such notification may endanger measures to protect public safety (including where notification would endanger the investigation of criminal offences arising from the security incident). In deciding whether a notification should be delayed or omitted in circumstances where notification may endanger national security, a Party should consider whether it would be reasonable in the circumstances to omit notification or whether instead a delayed notification would be more appropriate.

253. In the event of a security incident in which there is a significant risk of physical or non-physical harm to individuals, notification shall also be provided to the individual(s) affected by the incident, in order to allow them to protect their interests, although this is subject to exceptions. First, paragraph 7.b states that notification need not be provided if the Party has taken appropriate measures so that there is no longer a significant risk of harm. For example, no notification would be required where an e-mail containing sensitive personal information was accidentally sent to the wrong recipient and would have created a significant risk of harm without mitigation measures but was quickly and permanently deleted by the recipient upon request before it was further shared. Second, notification to the individual may be delayed or omitted under the conditions set out in paragraph 12.a.i – that is, notification "may be subject to the application of proportionate restrictions permitted under its domestic

legal framework, needed … to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned".

254. In general, Parties are encouraged to include in a notification under paragraph 7.b, where appropriate, information on the type of security incident, the type and volume of information that may have been compromised, the possible risks and the measures envisaged to be taken to mitigate possible harm, including measures to contain the incident. Given their supervisory function, and with a view to benefiting from expert advice on the handling of the incident, it may also be appropriate for the notifying Party to inform oversight authorities described in paragraph 14 of the incident and any mitigating measures.

255. In order to allow for a co-ordinated response and to support it in its own risk-mitigating efforts, the notified Party may request consultation and additional information concerning the incident and the response thereto from the notifying Party.

256. Paragraph 7.c provides required procedures for Parties to designate the authority or authorities to be notified under paragraph 7.b for the purposes of Chapter II, section 2.

Paragraph 8 – Maintaining records

257. Paragraph 8 requires Parties to "maintain records or have other appropriate means to demonstrate how an individual's personal data are accessed, used and disclosed in a specific case". The objective is for each Party to have effective means for demonstrating how the data of a specific individual have been accessed, used and disclosed in a specific case, in accordance with this article. Demonstrating compliance is important in particular for oversight purposes and as such contributes to accountability. While the precise means of demonstrating how data are processed is left to each Party to implement, Parties are encouraged to adapt their methods to the circumstances, taking into account the risks to the individuals concerned and the nature, scope, purposes and overall context of the processing.

258. For example, some Parties may decide to utilise automated recording of activities (logging) or other alternatives (such as handwritten records in the case of paper files). As noted above, the objective is to facilitate accountability but permit a degree of flexibility in terms of how a Party does so, consistent with other applicable obligations under Article 14. For example, Parties should maintain records or other documentation on access, use or disclosure in a manner that facilitates the work of oversight authorities.

Paragraph 9 – Onward sharing within a Party

259. Paragraph 9 provides that "[w]hen an authority of a Party provides personal data received initially under this Protocol to another authority of that Party, that other authority shall process it in accordance with this article, subject to paragraph 9.b". In other words, whenever personal data received under this Protocol is subsequently provided to another authority of the same Party – including to an authority of a constituent State or another similar territorial entity – such data must be processed in accordance with this article unless the exception in paragraph 9.b applies. Paragraph 9 also applies in the case of multiple instances of onward sharing.

260. Paragraph 9.b provides an exception to paragraph 9.a when a Party that is a federal State has taken a reservation to the obligations of this Protocol under Article 17, in accordance with the conditions set out therein. In line with paragraph 297 of this explanatory report, this exception accommodates "the difficulties federal States may face as a result of their characteristic distribution of powers between central and regional authorities". See also paragraph 316 of the explanatory report to the Convention. Paragraph 9.b therefore states that, where a Party has made a reservation under Article 17, it may still provide personal data initially received under this Protocol to its constituent States or other similar territorial entities provided that the Party has in place measures in order that the receiving authorities continue to effectively protect the data by providing for a level of protection of the data comparable to that afforded by this article. A Party's failure to have "in place measures in order that the receiving authorities continue to effectively protect the data by providing for a level of protection of the data comparable to that afforded by this article" may, depending on the seriousness, grounds and circumstances of the failure to meet this requirement, constitute a material or systematic breach under paragraph 15 of Article 14.

261. Paragraph 9.c provides that in case of indications of improper implementation of this paragraph by another Party, the transferring Party may request consultation with that other Party and relevant information about those indications with a view to clarifying the situation.

Paragraph 10 – Onward transfer to another State or international organisation

262. Pursuant to paragraph 10.a, a Party may transfer personal data received under the Protocol "to another State or international organisation only with the prior authorisation of the transferring authority or, for purposes of Chapter II, section 2, the authority or authorities designated in paragraph 10.b". This type

of protective measure is a common condition of transfers to assist foreign partners in the criminal law-enforcement context (for example pursuant to mutual assistance treaties or police-to-police co-operation), and this approach is carried over to this paragraph also as a means of protecting personal data transferred under this Protocol.

263. Paragraph 10.b provides that each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities designated to provide authorisation under paragraph 10.a for the purposes of transfers under Chapter II, section 2, which may subsequently be modified.

264. Obtaining authorisation for an onward transfer may entail an individualised request being sent from the receiving Party's authorities to the authorities of the transferring Party for authorisation to transfer specifically identified personal data to a specific third country or international organisation. However, paragraph 10.a does not prevent Parties from prescribing rules for onward transfers in advance (for example via written agreement or other arrangements). Paragraph 10.a is also without prejudice to the ability of a Party to place other conditions on the use by the recipient of the data (for example placing limitations on the extent to which the receiving Party can use or disseminate the personal data in order to avoid prejudice to the investigation of the transferring Party) in accordance with the specific provisions of Chapter II.

265. When determining whether to grant authorisation to a transfer under paragraph 10, the transferring or designated authority is encouraged to take due account of all relevant factors, including the seriousness of the criminal offence, the purpose for which the data were originally transferred, any applicable conditions relating to the original transfer and whether the third country or international organisation ensures an appropriate level of protection of personal data.

Paragraph 11 – Transparency and notice

266. Paragraph 11.a imposes certain transparency and notice requirements on Parties with regard to the items specified in paragraphs 11.a.i to iv. These transparency and notice requirements help individuals understand how Parties may process their data. These requirements also inform individuals about access, rectification and redress available.

267. Each Party has flexibility as to whether such notice and transparency is provided through the publication of general notices to the public – for instance on a governmental website – or via personal notice to the individual whose personal data the Party has received. Notice should be accessible without difficulty and easily understandable. Whether general or personal notice is provided, the following information must be included: (i) the legal basis for processing and the purpose(s) of processing, including the purposes of anticipated or usual disclosures; (ii) retention or review periods pursuant to paragraph 5 of this article, as applicable; (iii) recipients or categories of recipients to whom the data are disclosed; and (iv) access, rectification and judicial and non-judicial remedies available.

268. Under paragraph 11.b, when personal notice is provided to the individual whose data the Party has received, the notice and transparency requirement of paragraph 11.a may be subject to reasonable restrictions pursuant to the conditions set forth in paragraph 12.a.i of this article. For instance, within the context of criminal justice matters there may be legitimate circumstances in which the provision of notice may be delayed or omitted. These circumstances are referenced in paragraph 12.a.i and described in paragraph 272 of this explanatory report. Situations may also arise where the amount of detail provided in the general notice may be limited, depending on the sensitivity of the information.

269. Paragraph 11.c provides a basis for Parties to balance the interest in transparency with the need for confidentiality in criminal justice matters. It provides that where the domestic legal framework of the transferring Party requires personal notice to the individual whose data have been provided to another Party under this Protocol, the transferring Party shall take measures so that the receiving Party is informed at the time of transfer regarding this requirement and of appropriate contact information. The transferring Party shall not give notice to the individual if the receiving Party has requested, where the conditions for restrictions as set out in paragraph 12.a.i apply, that the provision of the data be kept confidential. Once such conditions for restrictions no longer apply and the personal notice may be provided, the receiving Party shall take measures so that the transferring Party is informed that notice may be given. This may include a periodic review of the need for such restrictions. If it has not yet been informed, the transferring Party is entitled to make requests to the receiving Party which will inform the transferring Party whether to maintain the restriction.

Paragraph 12 – Access and rectification

270. Paragraph 12.a requires each Party to ensure that any individual whose personal data have been received under this Protocol is entitled to seek and obtain, in accordance with processes established in its domestic legal framework and without undue delay, access to such data (subject to possible restrictions) and, where such data are inaccurate or have been improperly processed, rectification. The phrase "in accordance with processes established in its domestic legal framework" gives Parties flexibility regarding the manner of how access and rectification may be sought and obtained, and is intended to refer to processes established in, for example, applicable laws, regulations, rules (such as jurisdictional rules) and policies, as well as applicable rules of evidence. In some legal systems, an individual will need to pursue access and rectification administratively before seeking judicial remedies.

271. Paragraph 12.a.i provides that in the case of a request for access, an individual is entitled to obtain a written or electronic copy of the documentation that contains the individual's personal data and available information indicating the legal basis and purpose(s) of processing, retention and recipients or categories of recipients of the data ("access"), as well as information regarding available options for redress pursuant to paragraph 13. This may also allow the individual to confirm whether (or not) their personal data have been received under this Protocol, and have been or are being processed. Providing documentation containing available information that indicates the legal basis and purpose(s) of processing will assist the individual in assessing whether the personal data are being processed in accordance with applicable law. Many Parties may already provide a framework for such access through their privacy, freedom of information or access to governmental records laws.

272. The ability to obtain such access in a particular case may be subject to proportionate restrictions permitted under a Party's domestic legal framework, "needed, at the time of adjudication, to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned". The rights and freedoms of others may, for instance, include the privacy of other individuals whose personal data would be revealed in the event access is granted. Important objectives of general public interest may, for instance, include the protection of national security and public safety (for example information on potential terrorist threats or serious risks to law-enforcement officials); the prevention, detection, investigation or prosecution of criminal offences; and avoiding prejudice to official inquiries, investigations and proceedings.

In a manner similar to the description of proportionality in paragraph 146 of the explanatory report to the Convention, "proportionate restrictions" in this context are expected to be implemented by each Party in accordance with the relevant principles of its domestic legal framework. For Parties to the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5) or to Protocol CETS No. 223 amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, proportionality will be derived from the requirements of those conventions. Other Parties will apply related principles of their domestic legal framework that reasonably limit the ability to obtain access to protect other legitimate interests. As stated above, proportionate restrictions must protect the rights and freedoms of others or protect important objectives of general public interest and give due regard to the "legitimate interests of the individual concerned". The phrase "legitimate interests of the individual concerned" was considered by the drafters to include the individual's rights and freedoms. In the case where these grounds for restrictions are invoked, the requested authority is encouraged to document such a decision for the purpose of paragraph 14. Parties should also consider whether partial access may be granted where the grounds for any restriction (for example to protect classified or confidential commercial information) only apply to certain parts of the information.

273. Where other provisions of this article allow for restrictions under conditions set out in paragraph 12.a.i, "at the time of adjudication" is intended to refer, in the case of paragraph 7, to the time of notification of a security incident; in the case of paragraph 11.b, to the time of providing personal notice; and in the case of 11.c, to the time a Party requests confidentiality.

274. According to paragraph 12.a.ii, each Party shall ensure that any individual, whose data have been received under this Protocol, is entitled to seek and obtain, in accordance with processes established in its domestic legal framework and without undue delay, rectification when the individual's personal data are inaccurate or have been improperly processed. Rectification shall include – as appropriate and reasonable considering the grounds for rectification and the particular context of processing – correction, supplementation (for example through flagging or by providing additional or corrective information), erasure or anonymisation, restriction of processing or blocking. In this regard, the drafters considered that erasure or anonymisation is the appropriate and reasonable course of action if the data are processed in violation of paragraph 5. In the case of a violation of paragraph 2, it may also be appropriate for the Party to restrict processing; however, this will ultimately depend on the particular

context (for example the need to maintain personal data for the purpose of evidence). When data are rendered anonymous, Parties should consider the risk of unauthorised re-identification and implement appropriate measures to minimise that risk. Parties are encouraged, when feasible, to notify the Party from which the data were received and other entities with whom the data have been shared of any rectification actions taken.

275. According to paragraph 12.b, if access or rectification is denied or restricted under paragraph 12.a, the Party shall provide to the individual, in written form which may be provided electronically, without undue delay, a response informing that individual of the denial or restriction. While the authority shall provide the grounds for such denial or restriction, a communication may be general (that is, without confirming or denying the existence of any relevant record) where needed in order not to undermine an objective under paragraph 12.a.i. Parties shall, however, ensure that the communication includes information about available options for redress.

276. Parties may charge a fee for obtaining access (for example the administrative cost of assembling and examining documents to which access has been sought). However, in order not to dissuade or discourage access, any charge should be limited to what is reasonable and not excessive given the resources involved. In order to facilitate the exercise of the rights set out in paragraph 12.a, Parties are encouraged to allow individuals to request a representative to assist in seeking and obtaining the measures described therein, or to lodge a request and/or complaint on his or her behalf. In those circumstances, the notice pursuant to paragraph 11.a as well as the information obtained in response to a request for access pursuant to paragraph 12.a.i. may refer to this possibility. However, such representation must be in accordance with applicable domestic legal requirements of the Party in which such measures are sought, or the request and/or complaint is lodged as described above, including the rules governing the conditions under which persons or entities may represent legal interests of others (for example, in some domestic legal systems, the rules governing the power of attorney).

Paragraph 13 – Judicial and non-judicial remedies

277. Paragraph 13 provides that "[e]ach Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of this article". It is left to each Party to determine the type of remedies for violations of the provisions of this article, and it is not required that each type of remedy be available for every violation of this article. The remedies provided

must be effective in addressing violations of this article. Parties may include compensation as a remedy, where appropriate, for physical or non-physical harm that the claimant has established has resulted from the violation.

Paragraph 14 – Oversight

278. Paragraph 14 requires Parties to have "in place one or more public authorities that exercise, alone or cumulatively, independent and effective oversight functions and powers with respect to the measures set forth in this article". The provision leaves Parties flexibility in how to implement this requirement. Some Parties may create specialised data protection authorities, while others may choose to exercise oversight cumulatively through more than one authority, whose functions may overlap. This reflects differences in Parties' constitutional, organisational and administrative structures. In some Parties, these oversight authorities may be located within the governmental components whose activities they are overseeing, and their budgets may be part of the component's overall budget. In such a case, these authorities should enjoy independence to carry out their oversight responsibilities effectively.

279. The drafters considered that a number of elements contribute to independent and effective oversight functions and powers. The authorities should perform their tasks and exercise their powers impartially; they should enjoy the ability to act free from external influence that could interfere with the independent exercise of their powers and functions; in particular such authorities should not be subject to instructions, in a particular case, as to the exercise of their investigation powers and/or the taking of corrective action; and, finally, it is important that the authorities have the necessary skills, knowledge and expertise to perform their duties, and receive appropriate financial, technical and human resources for the effective performance of their functions.

280. These authorities' functions and powers shall "include investigation powers, the power to act upon complaints and the ability to take corrective action". The drafters considered that investigation powers should include the power to obtain the information necessary for the performance of their tasks, including, subject to appropriate conditions, access to records maintained pursuant to paragraph 8. Corrective action may include issuing warnings for non-compliance or directions on how to bring data processing operations into compliance (for example by requiring the implementation of additional security measures to limit access to data or the rectification of personal data), requiring the (temporary) suspension of certain processing operations or referring the matter to other authorities (for example inspectors general,

public prosecutors, investigative judges or legislative bodies). Such corrective action may be taken on authorities' own initiative or upon complaints made by individuals relating to the processing of their personal data.

281. Parties are encouraged to promote co-operation between their respective oversight authorities. Consultations between the Parties' respective authorities when carrying out their oversight functions under this article may take place as appropriate. This may include the exchange of information and best practices.

Paragraph 15 – Consultation and suspension

282. Paragraph 15 governs when, under Article 14, a Party may suspend the transfer of personal data under this Protocol to another Party when Parties are proceeding under paragraph 1.a of Article 14. Paragraph 15 makes clear that in light of the important law-enforcement purposes of this Protocol, such suspensions should only occur under strict conditions and pursuant to the specific procedures described therein. The purpose of the data protection provisions of this article is to provide appropriate safeguards for the protection of personal data, including in case of onward sharing within a Party and onward transfers. The drafters considered that the safeguards of this article and their effective implementation are essential and thus considered it important to provide for suspension of transfers of personal data for certain situations. Therefore, a Party may suspend the transfer of personal data under this Protocol to another Party if it has substantial evidence of a systematic or material breach of the terms of this article, or that a material breach is imminent. While the "substantial evidence" requirement does not oblige a Party to demonstrate a systematic or material breach beyond doubt, it may not suspend transfers based on a mere suspicion or conjecture either. Rather, the Party's determination must have substantial support in credible factual evidence. A "material breach" means a significant violation of a material obligation under this article. This may include the failure to provide for a required safeguard of this article in a Party's domestic legal framework. The drafters recognised that suspension is also available on the grounds of systematic breaches – for example frequently recurring violations of the safeguards of this article. The drafters further recognised that a failure to apply certain safeguards in relation to the processing of personal data in an individual case will, in the absence of a material breach, not provide a sufficient ground for invoking this provision, as the individual concerned should be able to address such violations through effective non-judicial and judicial remedies pursuant to paragraph 13 of Article 14.

283. Paragraph 15 further provides that a Party "shall not suspend transfers without reasonable notice, and not until after the Parties concerned have engaged in a reasonable period of consultation without reaching a resolution". This consultation requirement recognises that suspending critical law-enforcement transfers should only be undertaken after providing the other Party with a reasonable opportunity to clarify the situation or to address stated concerns. At the outset of such consultation, the Party invoking paragraph 15 may request the other Party to provide relevant information. However, as recognised in paragraph 15, the Party invoking this paragraph must have substantial evidence of a material or systematic breach or imminent material breach beforehand; therefore, the consultation mechanism should not be used in order to gather further evidence where a breach is merely suspected. Data transfers under this Protocol may only be suspended following reasonable notice and a reasonable period of consultation without reaching resolution. However, a Party may provisionally suspend transfers in the event of a systematic or material breach that poses a significant and imminent risk to the life or safety of, or a significant and imminent risk of substantial reputational or monetary harm to, a natural person. This includes a significant and imminent risk of bodily harm or to the health of a natural person. In these cases, the Party shall notify and commence consultations with the other Party immediately after provisionally suspending transfers. The drafters considered that the provisional suspension should generally be limited to those transfers directly related to the exigency justifying the provisional suspension.

284. If the suspending Party fulfils the conditions set out in paragraph 15, it may suspend transfers and the other Party may not reciprocate. However, if the other Party has substantial evidence that suspension by the suspending Party was contrary to the terms of paragraph 15, it may reciprocally suspend data transfers to the suspending Party. In this context, the term "substantial evidence" has the same meaning as it does with respect to the initial suspension by the suspending Party. Suspension by the suspending Party would be contrary to the terms of paragraph 15, for instance, if the suspending Party did not have "substantial evidence", the breach was neither "systematic" nor "material" or the suspending Party failed to satisfy the procedural requirements for suspension, in particular those related to consultations.

285. Finally, paragraph 15 provides that the "suspending Party shall lift the suspension as soon as the breach justifying the suspension has been remedied" and that "any reciprocal suspension shall be lifted at that time". A similar rule to that applied in Article 24, paragraph 4, applies in the context of suspension

under this paragraph. That is, paragraph 15 provides that "[a]ny personal data transferred prior to suspension shall continue to be treated in accordance with this Protocol".

286. Parties are encouraged to make public or formally notify service providers and entities to whom requests or orders may be directed under Chapter II, section 2, of any suspension or provisional suspension under this paragraph. Such communication can be important in order to effectively suspend transfers of personal data to a Party that is in material or systematic breach of Article 14 but also to ensure that service providers and entities do not restrict the transfer of information or evidence under this Protocol based on the mistaken belief that a Party is subject to this suspension provision.

287. Although paragraph 15 provides for specific procedures related to consultation and suspension of personal data transfers on data protection grounds, the procedures in paragraph 15 are not intended to affect consultations under Article 23, paragraph 1, or rights of suspension that may be applicable under international law with respect to other articles of this Protocol.

Chapter IV – Final provisions

288. The provisions contained in this chapter are, for the most part, based both on the "Model final clauses for conventions, additional protocols and amending protocols concluded within the Council of Europe", which were adopted by the Committee of Ministers at the 1291st meeting of the Ministers' Deputies in July 2017, and the final clauses of the Convention. As some of the articles under this chapter either use the standard language of the model clauses or are based on long-standing treaty-making practice at the Council of Europe, they do not call for specific comments. However, certain modifications of the standard model clauses and deviation from the final provisions of the Convention require some explanation.

Article 15 – Effects of this Protocol

289. Paragraph 1.a of Article 15 incorporates Article 39, paragraph 2, of the Convention. As recognised in paragraph 312 of the explanatory report to the Convention, this paragraph provides that Parties are free to apply agreements that already exist or that may in the future come into force. This Protocol, like the Convention, generally provides for minimum obligations; therefore, this paragraph recognises that Parties are free to assume obligations that are more specific in addition to those already set out in this Protocol, when establishing

their relations concerning matters dealt with therein. However, Parties must respect the objectives and principles of the Protocol when so doing and therefore cannot accept obligations that would defeat its purpose.

290. Paragraph 1.b of this article also acknowledges the increased integration of the European Union (EU) since the Convention was opened for signature in 2001, particularly in the areas of law enforcement and judicial co-operation in criminal matters as well as data protection. It, therefore, permits EU member States to apply European Union law that governs matters dealt with in this Protocol between themselves. The drafters intended European Union law to include measures, principles and procedures provided for in the EU legal order, in particular laws, regulations or administrative provisions as well as other requirements, including court decisions. Paragraph 1.b is intended, therefore, to cover the internal relations between EU member States and between EU member States and institutions, bodies and agencies of the EU. If there is no European Union law relating to a matter falling within the scope of this Protocol, this Protocol would continue to govern that matter between Parties that are EU member States.

291. Paragraph 1.c makes clear that paragraph 1.b does not affect the full application of this Protocol between Parties that are members of the EU and other Parties. Paragraph 1.b is not intended, therefore, to have any effect beyond the internal relations of the EU as described in paragraph 290 above; this Protocol applies in full between Parties that are EU member States and other Parties. The drafters considered such a provision vital to ensure that Parties that are not EU member States would receive all benefits of this Protocol in their relations with Parties that are EU member States. For example, the drafters discussed that an EU member State that receives information or evidence from a non-EU Party would have to seek the consent of the non-EU Party before transferring the information or evidence to another EU Party, consistent with Article 14, paragraph 10. Similarly, paragraph 1.a of this article would fully apply between Parties that are EU member States and other Parties that are not.

292. Paragraph 2 of Article 15 incorporates Article 39, paragraph 3, of the Convention. Similar to the Convention, as explained in paragraph 314 of the Convention's explanatory report, this Protocol does not purport to address all outstanding issues relating to forms of co-operation between Parties or between Parties and private entities related to cybercrime and to the collection of evidence in electronic form of criminal offences. Therefore, paragraph 2 of Article 15 was inserted to make plain that this Protocol only affects what

it addresses. Left unaffected are other rights, restrictions, obligations and responsibilities that may exist but that are not dealt with by this Protocol.

293. Article 15 does not contain a provision analogous to Article 39, paragraph 1, of the Convention. That provision in the Convention explained that the purpose of the Convention was to supplement applicable bilateral treaties or arrangements between the Parties, including certain extradition and mutual assistance treaties. This Protocol does not contain any extradition provisions, and it has many provisions that are not mutual assistance provisions. As explained more thoroughly in Article 5 and in its accompanying explanatory report, each section of co-operation measures in Chapter II interacts in different ways with mutual assistance treaties. Therefore, the drafters concluded that they need not include a provision similar to Article 39, paragraph 1.

Article 16 – Signature and entry into force

294. Article 16 permits all Parties to the Convention to sign and become Parties to this Protocol. Unlike the First Protocol (Article 11), this Protocol does not foresee a procedure for accession to this Protocol. A State wishing to sign and become a Party to this Protocol will need to become a Party to the Convention first.

295. Paragraph 3 provides that this "Protocol 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 Parties to the Convention have expressed their consent to be bound by this Protocol". While the Convention provided in Article 36, paragraph 3, that at least three out of the five Parties had to be member States of the Council of Europe for the Convention to enter into force, such a requirement is not included here given that this is an additional protocol to a convention and that all Parties should have the same right to apply this Protocol as soon as a minimum number of five Parties to the Convention have expressed their consent to be bound. This follows the approach of Article 10 of the First Protocol.

296. Paragraph 4 describes the process for the coming into force of this Protocol for those Parties to the Convention that express their consent to be bound by this Protocol subsequent to its entry into force under paragraph 3. This follows the approach of Article 36, paragraph 4, of the Convention.

Article 17 – Federal clause

297. Similar to the federal clause provided in Article 41 of the Convention, Article 17 of this Protocol contains a federal clause permitting a Party that is a

federal State to take a reservation "consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities". The goal of Article 17 is the same as that of Article 41 of the Convention. That is, as stated in paragraph 316 of the explanatory report to the Convention, "to accommodate the difficulties federal States may face as a result of their characteristic distribution of power between central and regional authorities".

298. Federal States are permitted to take a reservation to the obligations in Chapter II of the Convention (establishment of domestic criminal offences and domestic procedural measures), to the extent that the measures do not fall within the power of a federal State's central government to regulate. However, federal States are required to be able to provide international co-operation to other Parties under Chapter III of the Convention.

299. Although this Protocol provides for international co-operation rather than domestic measures, the negotiators recognised that a federal clause is still needed in this Protocol. While the Convention provided no federalism reservation for mutual assistance, the majority of this Protocol's measures do not operate in the same manner as traditional mutual assistance. This Protocol provides a number of co-operation measures that are more efficient than traditional mutual assistance and which do not necessarily require central government involvement. In particular, this Protocol introduces two measures, Articles 6 and 7, in which competent authorities in one Party may seek co-operation directly from private companies in another Party. These measures require certain procedural steps that a federal State may have difficulty requiring competent authorities from constituent States or territorial entities to comply with. For instance, Article 7 provides that a Party may, through notification to the Secretary General, require that authorities from other Parties notify a designated governmental authority simultaneously when transmitting an order to a service provider seeking subscriber information. Other articles contain requirements to take legislative or other measures that a federal State may be unable to require its constituent States or other similar territorial entities to enact. Finally, this Protocol contains detailed data protection provisions, whereas the Convention did not. For example, in the United States, under its constitution and fundamental principles of federalism, its constituent States enact their own criminal and criminal procedural laws (separate from federal laws); establish their own courts, prosecutors and police; and investigate and prosecute State criminal offences. State competent authorities are independent from and not subordinate to federal authorities.

300. Should authorities of a federal State's constituent State or similar territorial entity seek the forms of co-operation provided under this Protocol, it may be the case that (i) they are operating under different procedural and privacy laws than those under which the central government authorities operate; (ii) they do not answer to the central government in terms of organisational hierarchy; or (iii) the central government does not have the legal power to direct their actions. In such situations, there could only be the assurance that a constituent State or similar territorial entity would fulfil the requirements of this Protocol – those related to seeking information or evidence, as well as those relating to the subsequent handling of such information or evidence – if (i) it applies them itself, or (ii) if its authorities sought co-operation via, or with the participation of, central government authorities which would see to their fulfilment (for example via mutual assistance or the 24/7 point of contact, or with the participation of the central government in a JIT).

301. In view of these considerations, paragraph 1 provides a reservation possibility for Parties that are federal States. Such Parties may reserve the right to assume obligations under this Protocol consistent with their fundamental principles governing the relationship between their central government and constituent States or other similar territorial entities, subject to paragraphs 1.a to c, which limit the scope of such a reservation. Under paragraph 1.a, the central government of a federal State invoking this reservation is required to apply all of the terms of this Protocol (subject to available reservations and declarations). With respect to data protection obligations under this Protocol, for Parties proceeding under Article 14, paragraph 1.a, this includes the obligations in Article 14, paragraph 9.b, regarding onward sharing with constituent States or other similar territorial entities (see explanatory report, paragraph 260) where a federal authority has sought information under this Protocol, either for its own purposes or on behalf of an authority at the sub-federal level, and subsequently shares this information with such authority at the sub-federal level. In addition, paragraph 1.b provides that, similar to Article 41, paragraph 1, of the Convention, such a reservation shall not affect obligations of that federal State Party to provide for co-operation sought by other Parties in accordance with the provisions of Chapter II. Finally, under paragraph 1.c, notwithstanding a federal State's reservation, Article 13 of this Protocol – which requires, in accordance with Article 15 of the Convention, protection of human rights and liberties under domestic law – applies to the federal State's constituent States or similar territorial entities in addition to the central government under paragraph 1.a.

302. Paragraph 2 provides that, if a federal State takes a reservation under paragraph 1, and the authorities of a constituent State or similar territorial entity in that Party seek co-operation directly from an authority, provider or entity in another Party, such other Party "may prevent authorities, providers or entities in its territory from co-operating in response" thereto. The other Party may determine in what manner to prevent its authorities or providers or entities in its territory from co-operating. There are two exceptions to the power of another Party to prevent co-operation.

303. First, paragraph 2 provides that co-operation may not be prevented by such other Party if, because the constituent State or other similar territorial entity fulfils the obligations of this Protocol, the federal State Party concerned has "notifie[d] the Secretary General of the Council of Europe that a constituent State or other similar territorial entity applies the obligations of this Protocol applicable to that federal State". The term "obligations of this Protocol applicable to that federal State" means that an authority of a constituent State or similar territorial entity may not be subjected to any requirement that the central government is not subject to, such as due to an applicable reservation. If the federal State has made this notification to the Secretary General with respect to a particular constituent State, another Party is required to provide for execution of an order or request from that State to the same extent as if it had been received from authorities of the central government. Of course, the requirements and procedures contained in each co-operation measure of Chapter II still apply to requests or orders submitted by such constituent States or similar territorial entities, and compliance with such requirements is necessary. This paragraph requires that the Secretary General of the Council of Europe shall set up and keep updated a register of such notifications. Parties are encouraged to provide the Secretary General with updated information.

304. Second, under paragraph 3, if a request or order of a constituent State or other similar territorial entity has been submitted via the central government or, under Article 12, pursuant to a joint investigative team agreement that has been entered into with the participation of the central government, another Party may not prevent authorities, providers or entities in its territory from transferring information or evidence pursuant to the terms of this Protocol on the grounds that co-operation is being sought by a constituent State or similar territorial entity of a federal State that has taken the reservation in paragraph 1. This is because when the request or order has been submitted via the central government or the joint investigative team agreement is entered into with the participation of the central government, it is the central government that

is required to "provide for the fulfilment of the applicable obligations of the Protocol". Because the central government is submitting the request or order (or participating in the JIT), it has the opportunity and obligation to verify that the requirements of this Protocol with respect to such measures are satisfied. For example, if, under Article 7, paragraph 5.a, another Party must be notified of the transmission of an order seeking subscriber information, the central government is obligated to provide this notification. With respect to data protection (for Parties proceeding under Article 14, paragraph 1.a), if a constituent State or other similar territorial entity seeks co-operation through the central government, the central government provides the data to the constituent State or other similar territorial entity and must apply the requirements set forth in Article 14, paragraph 9.b (onward sharing within a Party). That is, the central government must have in place measures in order that the receiving authorities continue to effectively protect the data by providing for a level of protection comparable to that afforded by Article 14. The authorities of a constituent State or similar territorial entity that seek and receive personal data in this manner are otherwise not obligated to apply Article 14. If the Parties concerned are applying another agreement or arrangement described in Article 14, paragraphs 1.b or 1.c, the applicable terms of such agreement or arrangement shall apply.

305. Paragraph 4 has nearly the same text and the same effect as in Article 41, paragraph 3, of the Convention. Thus, with regard to provisions of the Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities (unless notification has been provided to the Secretary General of the Council of Europe in accordance with paragraph 2 of this article), the central government of the federal State is required to (i) inform the authorities of its constituent States or other similar territorial entities of the provisions of this Protocol; and (ii) give "its favourable opinion, encouraging them to take appropriate action to give them effect", which encourages the constituent States or similar territorial entities to fully apply this Protocol. For this Protocol, this is also intended to eventually permit such constituent States or other similar territorial entities to be notified under paragraph 2 of this article.

Article 18 – Territorial application

306. Article 38 of the Convention permits Parties to specify the territory or territories to which the Convention would apply. Article 18 of this Protocol automatically applies this Protocol to territories specified by a Party under

Article 38, paragraphs 1 or 2, of the Convention, to the extent such declaration has not been withdrawn under Article 38, paragraph 3, of the Convention. The drafters considered that it would be best if the same territorial scope of the Convention and this Protocol apply as the default rule.

307. Paragraph 2 of this article provides that "[a] Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that this Protocol shall not apply to one or more territories specified in the Party's declaration under Article 38, paragraphs 1 and/or 2 of the Convention". According to paragraph 3, Parties may withdraw the declaration under paragraph 2 of this article, according to the procedures specified. Withdrawing the declaration in paragraph 2 would have the effect of applying this Protocol to additional territories that were covered under the Convention but to which this Protocol had previously not been applied.

308. This article does not permit applying this Protocol to territories not covered by the Convention.

Article 19 – Reservations and declarations

309. This article provides for a number of reservation possibilities. Given the global reach of the Convention and the aim of achieving the same level of membership in this Protocol, such reservations enable Parties to the Convention to become Parties to this Protocol, while permitting such Parties to maintain certain approaches and concepts consistent with their domestic law, fundamental legal principles or policy considerations, as applicable.

310. The possibilities for reservations are restricted in order to secure to the greatest possible extent the uniform application of this Protocol by the Parties. Thus, no other reservations may be made than those enumerated. In addition, reservations may only be made by a Party to the Convention at the time of signature of this Protocol or upon deposit of its instrument of ratification, acceptance or approval.

311. As in the Convention, the reservations in this Protocol exclude or modify the legal effect of obligations set forth in this Protocol (see paragraph 315 of the explanatory report to the Convention). In this Protocol, reservations are permitted to exclude entire forms of co-operation. Specifically, Article 7, paragraph 9.a, permits a Party to reserve the right not to apply Article 7 in its entirety. Reservations are also permitted to exclude co-operation for entire articles with respect to certain types of data. Specifically, Article 7, paragraph 9.b, permits a Party to reserve the right not to apply Article 7 to

certain types of access numbers if disclosure of those access numbers would be inconsistent with the fundamental principles of its domestic legal system. Similarly, Article 8, paragraph 13, permits a Party to reserve the right not to apply Article 8 to traffic data.

312. Article 19 also refers to declarations. Similar to the Convention, through declarations in this Protocol, the Parties are permitted to include certain specified additional procedures which modify the scope of the provisions. Such additional procedures aim at accommodating certain conceptual, legal or practical differences, which are justified given the global reach of the Convention and aspiring equal reach of this Protocol. The enumerated declarations fall into two general categories.

313. Several declarations permit a Party to declare that certain powers or measures must be carried out by particular authorities or co-operation transmitted through particular channels. This is the case for Article 10, paragraph 9 (permitting a declaration that requests may be sent to authorities in addition to the central authority); Article 12, paragraph 3 (central authority must be a signatory to, or otherwise concur in, the JIT agreement); Article 8, paragraph 11 (a declaring Party may require that other Parties' requests under this article must be transmitted by their central authorities or other mutually determined authority).

314. A second category of declarations permits Parties to require separate or additional procedural steps for certain measures of co-operation in order to comply with domestic law or avoid overburdening authorities. For instance, Article 7, paragraph 8, and Article 9, paragraph 1.b, permit a Party to make declarations to require other Parties to take particular procedural steps with respect to subscriber information. Article 7, paragraphs 2.b and 5.a, Article 8, paragraph 4, and Article 9, paragraph 5, permit additional procedural steps to provide additional safeguards or to comply with domestic law. The effects of declarations are not intended to be reciprocal. For instance, if a Party makes a declaration under Article 10, paragraph 9 – that is, that requests under this article may be sent to authorities in addition to its central authority – other Parties may address requests to the additional authorities of the declaring Party, but the declaring Party may only address requests to the central authorities of other Parties unless they also make such a declaration.

315. Declarations listed under paragraph 2 of this article must be made at the time of a Party's signature or when depositing its instrument of ratification,

acceptance or approval. In contrast, declarations listed under paragraph 3 may be made at any time.

316. Paragraph 3 requires Parties to notify the Secretary General of the Council of Europe of any declarations, notifications or communications referred to in Article 7, paragraphs 5.a and 5.e, and Article 8, paragraphs 4 and 10.a and b, Article 14, paragraphs 7.c and 10.b, and Article 17, paragraph 2, of this Protocol according to the terms specified in those articles. For example, under Article 7, paragraph 5.e, a "Party shall, at the time when notification to the Secretary General of the Council of Europe under paragraph 5.a is first given, communicate to the Secretary General the contact information of that authority".

Parties shall furthermore communicate to the Secretary General of the Council of Europe, the "authorities" referred to in Article 8, paragraphs 10.a and b. The Secretary General has been directed to set up and keep updated a register of these authorities designated by the Parties, and the Parties are directed to ensure that the details they provide for the register are correct at all times (see Article 7, paragraph 5.f, and Article 8, paragraph 12).

Article 20 – Status and withdrawal of reservations

317. Like Article 43 of the Convention, this article, without imposing specific time limits, requires Parties to withdraw reservations as soon as circumstances permit. In order to maintain some pressure on the Parties and to make them at least consider withdrawing their reservations, paragraph 2 authorises the Secretary General of the Council of Europe to periodically enquire about the prospects for withdrawal. This possibility of enquiry is current practice under several Council of Europe instruments and is reflected in Article 43, paragraph 3, of the Convention and Article 13, paragraph 2, of the First Protocol. The Parties are thus given an opportunity to indicate whether they still need to maintain their reservations in respect of certain provisions and to withdraw, subsequently, those which no longer prove necessary. It is hoped that over time Parties will be able to remove as many of their reservations as possible so as promote this Protocol's uniform implementation.

Article 21 – Amendments

318. Article 21 follows the same procedure as that foreseen for amendments in Article 44 of the Convention. This simplified procedure permits amendments without the need for negotiation of an amending Protocol should the need arise. It is understood that the results of the consultations with the Parties to

the Convention under paragraph 3 of this article are not binding on the Parties to the Protocol. As indicated in paragraph 323 of the explanatory report to the Convention, "[t]he amendment procedure is mostly thought to be for relatively minor changes of a procedural and technical character".

Article 22 – Settlement of disputes

319. Article 22 provides that the dispute mechanisms provided by Article 45 of the Convention also apply to this Protocol (see paragraph 326 of the explanatory report to the Convention).

Article 23 – Consultations of the Parties and assessment of implementation

320. Paragraph 1 of Article 23 provides that Article 46 of the Convention (Consultations of the Parties) is applicable to this Protocol. According to paragraph 327 of the explanatory report to the Convention, Article 46 created "a framework for the Parties to consult regarding implementation of the Convention, the effect of significant legal, policy or technological developments pertaining to the subject of computer- or computer-related crime and the collection of evidence in electronic form, and the possibility of supplementing or amending the Convention". The procedure was designed to be flexible and it was left to the Parties to decide how and when to convene. Following the entry into force of the Convention in 2004, the Parties began to convene on a regular basis as the "Cybercrime Convention Committee" (T-CY). Over time, the T-CY, established according to Article 46 and based on Rules of Procedure adopted by the Parties to the Convention, undertook assessments of the implementation of the Convention by the Parties, adopted guidance notes to facilitate a common understanding of the Parties as to the use of the Convention, and prepared the draft of the present Protocol. The procedures for the consultations of the Parties remain flexible and may therefore be adapted by the Parties to this Protocol as appropriate, to take into account needs that may arise from the implementation of this Protocol.

321. Similar to the Convention (see paragraph 327 of the explanatory report), consultations under Article 23 should "examine issues that have arisen in the use and implementation of the Convention, including the effects of declarations and reservations made". This could include consultations on and assessment of implementation of this Protocol by constituent States or similar territorial entities of federal States notified to the Secretary General of the Council of Europe under Article 17, paragraph 2, and for Parties that are members of the

EU to inform and consult with other Parties to this Protocol of applicable EU laws in relation to their use and implementation of this Protocol in relation to Article 15, paragraph 1.b. In addition to consultations through the T-CY under this article discussed in the following paragraph, Parties may engage in consultations on a bilateral basis. For federal States, these consultations and assessments would take place via their central government.

322. Paragraph 2 of Article 23 establishes specific procedures for reviewing the use and implementation of the Protocol within the broader framework established by Article 46 and the T-CY discussed above. Paragraph 2 provides that "Parties shall periodically assess the effective use and implementation of the provisions of this Protocol" and indicates that Article 2 of the Rules of Procedure established by the T-CY, as revised on 16 October 2020, will govern these assessments. These procedures are available on the T CY website. Because the T-CY has reviewed several provisions of the Convention and issued reports pursuant to these procedures, the drafters considered that these well-established procedures shall apply *mutatis mutandis* to the assessment of the provisions of this Protocol. In light of the additional obligations undertaken by the Parties to this Protocol and the unique co-operation measures it provides, the drafters determined that solely the Parties to this Protocol would conduct these assessments. In view of the relevant expertise necessary for the assessment of the use and implementation of some of the provisions of this Protocol, including on Article 14 on data protection, Parties may consider involving their subject-matter experts in the assessments.

323. While on the one hand, the rules for such assessments need to be predictable, actual experience may lead to a need to adapt these procedures, without requiring a formal amendment of this Protocol according to Article 21. Therefore, paragraph 2 establishes that the initial review of the procedures shall take place five years after entry into force of this Protocol, at which point the Parties may modify these procedures by consensus. The Parties may modify the procedures by consensus at any point after that initial review.

324. Given the relevance of the data protection safeguards contained in Article 14, the drafters considered that Article 14 should be assessed as soon as there is a sufficient record of co-operation under this Protocol to effectively review Parties' use and implementation of this provision. Paragraph 3, therefore, provides that the assessment of Article 14 shall commence once ten Parties to the Convention have expressed their consent to be bound by this Protocol.

Article 24 – Denunciation

325. Paragraphs 1 and 2 of Article 24 are similar to those of Article 47 of the Convention and require no further explanation. Paragraph 3 states that "[D]enunciation of the Convention by a Party to this Protocol constitutes denunciation of this Protocol". Given the emphasis of this Protocol on the sharing of information or evidence, which may include personal data, the drafters considered it prudent to add paragraph 4 to clarify that "[i]nformation or evidence transferred prior to the effective date of denunciation shall continue to be treated in accordance with this Protocol".

Guidance Notes

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[15]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[16] This is to ensure that new forms of crime would always be covered by the Convention.

15. See the mandate of the T-CY (Article 46 Budapest Convention).
16. Paragraph 36 of the Explanatory Report.

Guidance Note on the notion of "computer system"[17]

Article 1.a Budapest Convention on Cybercrime

1. Introduction

The T-CY at its 1st meeting (Strasbourg, 20-21 March 2006) discussed the scope of the definition of "computer system" in Article 1.a Budapest Convention in the light of developing forms of technology that go beyond traditional mainframe or desktop computer systems.

Since the time of the drafting of the Convention new devices were developed such as modern generation mobile phones or "smart" phones, PDAs, tablets, and others that produce, process or transmit data. There has thus been a need to discuss whether these new devices are included in the concept of "computer system" of the Budapest Convention.

T-CY, in 2006, agreed that these devices were covered by the definition of "computer system" of Article 1.a.

The present Guidance Note states this common understanding of the Parties as reflected in the report of the 1st meeting (document T-CY(2006)11).

2. Article 1.a. Budapest Convention on Cybercrime (CETS 185)

Text of the Convention

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;

Extract of the Explanatory Report

> 23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is

17. Adopted by the T-CY at its 8th Plenary (5-6 December 2012).

operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

24. A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.

3. T-CY statement on the notion of "computer system" (Article 1.a Budapest Convention)

Article 1.a of the Convention defines "computer system" as any "device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

The T-CY agrees that this definition includes, for example, modern mobile telephones which are multifunctional and have among their functions the capacity to produce, process and transmit data, such as accessing the Internet, sending e-mail, transmitting attachments, upload contents or downloading documents.

Similarly the T-CY recognises that personal digital assistants, with or without wireless functionality, also produce, process and transmit data.

The T-CY underlines that, when these devices perform such functions, they are processing "computer data" as defined by Article 1.b. Furthermore, the T-CY considers that when they perform these functions they create "traffic data" as defined by Article 1.d.

Therefore, in processing such data, they are acting as a "computer system" as defined in Article 1.a.

The T-CY agrees that this is consistent with the interpretation of "computer system" set forth in the Convention's Explanatory Report and that the Convention is intended to cover these devices in that capacity.

4. Conclusion

T-CY agrees that the definition of "computer system" in Article 1.a covers developing forms of technology that go beyond traditional mainframe or desktop computer systems, such as modern mobile phones, smart phones, PDAs, tablets or similar.

Guidance Note on provisions of the Budapest Convention covering botnets[18]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[19]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of botnets.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[20] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to botnets.

1. Relevant provisions of the Budapest Convention on Cybercrime (CETS 185)

The term "botnet' may be understood to indicate:

> "a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ("zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These "zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This "controlling' computer is also known as the "command-and-control centre"".[21]

18. Adopted by the 9th Plenary of the T-CY (4-5 June 2013).
19. See the mandate of the T-CY (Article 46 Budapest Convention).
20. Paragraph 36 of the Explanatory Report.
21. Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (com (2010) 517 final).

Computers may be linked for criminal or good purposes.[22] Therefore, the fact that botnets consist of computers that are linked is not relevant. The relevant factors are that the computers in botnets are used without consent and are used for criminal purposes and to cause major impact.

Botnets are covered by the following sections of the Convention, depending on what each botnet actually does. Each provision contains an intent standard ("without right", "with intent to defraud" etc.) which should be readily provable when botnets are involved.

Relevant Articles	Examples
Article 2 – Illegal access	The creation and operation of a botnet requires illegal access to computer systems.[23]
	Botnets may be used to illegally access other computer systems.
Article 3 – Illegal interception	Botnets may use technical means to intercept non-public transmissions of computer data to, from, or within a computer system.
Article 4 – Data interference	The creation of a botnet always alters and may damage, delete, deteriorate or suppress computer data. Botnets themselves damage, delete, deteriorate, alter or suppress computer data.
Article 5 – System interference	Botnets may hinder the functioning of a computer system. This includes distributed denial of service attacks.[24]
Article 6 – Misuse of devices	All botnets are devices as defined in Article 6 because they are designed or adapted primarily to commit the offences established by Articles 2 through 5.[25] Programmes themselves that are used for the creation and operation of botnets also fall under Article 6. Therefore, Article 6 criminalizes the production, sale, procurement for use, import, distribution or otherwise making available as well as the possession of devices such as botnets or programmes used for their creation or operation.

22. Networks of computers may be created voluntarily for a criminal purpose. The crimes committed by such networks are covered by the Convention but are not discussed in this Note.
23. See also Guidance Guidance Note 1 on the Notion of "Computer System".
24. See separate Guidance Note
25. Parties that take reservations to Article 6 must still criminalize the sale, distribution or making available of devices covered by this Article.

Relevant Articles	Examples
Article 7 – Computer-related forgery	Depending on the botnet's design, it may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Article 8 – Computer-related fraud	Botnets may cause one person to lose property and cause another person to obtain an economic benefit from the inputting, altering, deleting, or suppressing of computer data and/or interfering with the function of a computer system.
Article 9 – Child pornography	Botnets may distribute child exploitation materials.
Article 10 – Infringements related to copyrights and related rights	Botnets may illegally distribute data that is protected by intellectual property laws.
Article 11 – Attempt, aiding and abetting	Botnets may be used to attempt or to aid or abet several crimes specified in the treaty.
Article 13 – Sanctions	Botnets serve multiple criminal purposes some of which have serious impact on individuals, on public or private sector institutions or on critical infrastructure. A Party may foresee, however, in its domestic law a sanction that is unsuitably lenient for botnet-related crime, and it may not permit the consideration of aggravated circumstances attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Therefore, Parties should ensure, pursuant to Article 13, that criminal offences related to botnets "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. Parties may also consider aggravating circumstances, for example, if botnets affect a significant number of systems or attacks causing considerable damage, including deaths or physical injuries, or damage to critical infrastructure.

3. T-CY statement

The above list of Articles related to botnets illustrates the multi-functional criminal use of botnets and criminal provisions that may apply.

Therefore, the T-CY agrees that the different aspects of botnets are covered by the Budapest Convention.

Guidance Note on DDOS attacks[26]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[27]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of denial of service (DOS) and distributed denial of service (DDOS) attacks.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[28] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to DOS and DDOS attacks.

1. Relevant provisions of the Budapest Convention on Cybercrime (CETS 185)

Denial of service (DOS) attacks are attempts to render a computer system unavailable to users through a variety of means. These may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users. Distributed denial of service (DDOS) attacks are denial of service attacks executed by many computers at the same time. There are currently a number of common ways by which DOS and DDOS attacks may be conducted. They include, for example, sending malformed queries to a computer system; exceeding the capacity limit for users; and sending more e-mails to e-mail servers than the system can receive and handle.

DOS and DDOS attacks are covered by the following sections of the Convention, depending on what each attack actually does. Each provision contains an intent standard ("without right", "with intent to defraud," etc) which should be readily provable in DOS and DDOS cases.

---

26. Adopted by the 9th Plenary of the T-CY (4-5 June 2013).
27. See the mandate of the T-CY (Article 46 Budapest Convention).
28. Paragraph 36 of the Explanatory Report.

2. T-CY interpretation of the criminalisation of DDOS attacks

Relevant Articles	Examples
Article 2 – Illegal access	Through DOS and DDOS attacks a computer system may be accessed.
Article 4 – Data interference	DOS and DDOS attacks may damage, delete, deteriorate, alter or suppress computer data.
Article 5 – System interference	The objective of a DOS or DDOS attack is precisely to seriously hinder the functioning of a computer system.
Article 11 – Attempt, aiding and abetting	DOS and DDOS attacks may be used to attempt or to aid or abet several crimes specified in the treaty (such as Computer-related forgery, Article 7; Computer-related fraud, Article 8; Offences related to child pornography, Article 9; and Offences related to infringements of copyright and related rights, Article 10).
Article 13 – Sanctions	DOS and DDOS attacks may be dangerous in many ways, especially when they are directed against systems that are crucial to daily life - for example, if banking or hospital systems become unavailable. A Party may foresee in its domestic law a sanction that is unsuitably lenient for DOS and DDOS attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation. of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. Parties may also consider aggravating circumstances, for example, if DOS or DDOS attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure.

3. T-CY statement

The above list of Articles related to DOS and DDOS attacks illustrates the multi-functional criminal use of such attacks.

Therefore, the T-CY agrees that the different aspects of such attacks are covered by the Budapest Convention.

Guidance Note on Identity theft and phishing in relation to fraud[29]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[30]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of identity theft and phishing and similar acts[31] in relation to fraud.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[32] This is to ensure that new forms of crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to identity theft in relation to fraud and involving computer systems.

1. Identity theft and phishing

While there is no generally accepted definition nor consistent use of the term, identity theft commonly involves criminal acts of fraudulently (without his or her knowledge or consent) obtaining and using another person's identity information. The term "identity fraud" is sometimes used as a synonym, although it also encompasses the use of a false, not necessarily real, identity.

While personally identifiable information of a real or fictitious person may be misused for a range of illegal acts, the present Guidance Note focuses on identity theft in relation to fraud only.

This may entail the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name.

---

29. Adopted by the 9th Plenary of the T-CY (4-5 June 2013).
30. See the mandate of the T-CY (Article 46 Budapest Convention).
31. Similar acts to phishing are known under various names such as spear phishing, SMiShing, pharming and vishing.
32. Paragraph 36 of the Explanatory Report.

Related acts may include "phishing", "pharming", "spear phishing", "spoofing" or similar conduct, for example, to obtain password or other access credentials, often through email or fake websites.

Identity theft affects governments, businesses and citizens and causes major damage. It undermines confidence and trust in information technologies.

In many legal systems there is no specific offence of identity theft. Perpetrators of identity theft are normally charged with more serious offences (e.g. financial fraud). Obtaining a false identity normally implies a crime, such as the forgery of documents or the alteration of computer data. A false identity facilitates many crimes, including illegal immigration, trafficking in human beings, money laundering, drug trafficking, financial fraud against governments and the private sector, but is most generally seen in conjunction with fraud.

Conceptually, ID theft can be separated into three distinct phases:

- Phase 1 – The obtaining of identity information, for example, through physical theft, through search engines, insider attacks, attacks from outside (illegal access to computer systems, Trojans, keyloggers, spyware and other malware) or through the use of phishing and or other social engineering techniques.
- Phase 2 – The possession and disposal of identity information, which includes the sale of such information to third parties.
- Phase 3 – The use of the identity information to commit fraud or other crimes, for example by assuming another's identity to exploit bank accounts and credit cards, create new accounts, take out loans and credit, order goods and services or disseminate malware.

In conclusion: identity theft (including phishing and similar conduct) is generally used for the preparation of further criminal acts such as computer related fraud. Even if identity theft is not criminalised as a separate act, law enforcement agencies will be able to prosecute the subsequent offences.

2. T-CY interpretation of the criminalisation of identity theft in relation to fraud under the Budapest Convention

The Budapest Convention is focusing on criminal conduct and not specifically on techniques or technologies used. It does, therefore, not contain specific provisions on identity theft or phishing. However, full implementation of the Convention's substantive law provisions will allow States to criminalise conduct related to identity theft.

The Convention requires countries to criminalise conduct such as the illegal access to a computer system, the illegal interception of data, data interference, system interference, the misuse of devices and computer related fraud:

Phases	Articles of the Convention	Examples
Phase 1 – Obtaining of identity information	Article 2 – Illegal access	While a criminal is "hacking", circumventing password protection, keylogging or exploiting software loopholes, the computer may be illegally accessed in the acts of ID theft/phishing. Illegal access to computer systems is one of the most common offences committed in order to obtain sensitive infor mation such as identity information.
	Article 3 – illegal interception	ID theft often entails the use of keyloggers or other types of malware for the illegal interception of non-public transmissions of computer data to, from or within a computer system containing sensitive information such as identity information.
	Article 4 – Data interference	ID theft/phishing may involve damaging, deleting, deteriorating, altering or suppressing computer data. This is often done during the process of obtaining illegal access by installing a keylogger to obtain sensitive information.
	Article 5 – System interference	ID theft/phishing may involve hindering the functioning of a computer system in order to steal or facilitate the theft of identity information.
	Article 7 – Computer related forgery	ID theft/phishing may involve the inputting, altering, deleting, or suppressing of computer data with the result that inauthentic data is considered or acted upon as if it were authentic. Phishing is possibly the most common representation of computer related forgery (e.g. a forged web page of a financial institution) and as a consequence the most common illegal activity through which sensitive information is collected, such as identity information.

Phases	Articles of the Convention	Examples
Phase 2 – Possession and disposal of identity information	Article 6 – Misuse of devices	Stolen identity information – including passwords, access credentials, credit cards and others – may be considered "devices, including a computer program, designed and adapted for the purpose of committing any of the offences established in accordance with articles 2 through 5" of the Convention, or "a computer password, access code, or similar data by which the whole of any part of a computer system is capable of being accessed".
Phase 3 – Use of the identity information to commit fraud or other crimes	Article 8 – Computer related fraud	The use of a fraudulent identity by inputting, altering, deleting or suppressing computer data, and, or interfering with the function of a computer system will result in the exploitation of bank accounts or credit cards, in taking out loans and credit, or ordering goods and services, and thus causes one person to lose property and causes another person to obtain an economic benefit.
All Phases	Article 11 – Attempt, aiding and abetting	The obtaining, possession and disposal of identity information may constitute attempt, aiding and abetting of several crimes specified in the Convention.
	Article 13 – Sanctions	Identify theft serves multiple criminal purposes, some of which cause serious damage to individuals and public or private sector institutions. A Party may foresee, however, in its domestic law a sanction that is unsuitably lenient for identity theft, and it may not permit the consideration of aggravated circumstances. This may mean that Parties need to consider amendments to their domestic law. Therefore, Parties should ensure, pursuant to Article 13, that criminal offences related to identity theft "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanction. Parties may also consider aggravating circumstances, for example if identity theft affects a significant number of people or causes serious distress or exposes a person to danger.

3. T-CY statement

The T-CY agrees that the above illustrates the various scope and elements of identity theft and phishing and the criminal provisions that may apply.

Therefore, the T-CY agrees that the different aspects of such crimes are covered by the Budapest Convention.

Guidance Note on Critical information infrastructure attacks[33]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[34]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of critical information infrastructure attacks.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[35] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to critical information infrastructure attacks.

1. Relevant provisions of the Budapest Convention on Cybercrime (CETS 185)

Critical infrastructures can be defined as systems and assets, whether physical or virtual, so vital to a country that their improper functioning, incapacity or destruction would have a debilitating impact on national security and defence, economic security, public health or safety, or any combination of those matters. Countries define critical infrastructures differently. However, many countries consider critical infrastructures to include the energy, food, water, fuel, transport, communications, finance, industry, defence and governmental and public services sectors.

Critical infrastructures are often run by computer systems, including those known as industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems. In general, such systems are known as critical information infrastructures.

33. Adopted by the 9th Plenary of the T-CY (4-5 June 2013).
34. See the mandate of the T-CY (Article 46 Budapest Convention).
35. Paragraph 36 of the Explanatory Report.

According to private and governmental sources, a large but unknown number of attacks on critical information infrastructures worldwide takes place every year. These attacks use the same techniques as other electronic crime does. The difference is in the effect of such attacks on society: they may drain money from government treasuries, or shut down water systems, or confuse air traffic control, and so on.

Both current and future forms of critical information infrastructure attacks are covered by the following sections of the Convention, depending on the character of the attack. Each provision contains an intent standard ("without right", "with intent to defraud," etc) which should be taken into consideration when officials decide how to charge a crime.

2. T-CY interpretation of the criminalisation of Critical information infrastructure attacks

Relevant Articles	Examples
Article 2 – Illegal access	Critical information infrastructure attacks may access a computer system.
Article 3 – Illegal interception	Critical information infrastructure attacks may use technical means to intercept non-public transmissions of computer data to, from, or within a computer system.
Article 4 – Data interference	Critical information infrastructure attacks may damage, delete, deteriorate, alter or suppress computer data.
Article 5 – System interference	Critical information infrastructure attacks may hinder the functioning of a computer system; in fact, this may be their primary goal.
Article 7 – Computer-related forgery	Critical information infrastructure attacks may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Article 8 – Computer-related fraud	Critical information infrastructure attacks may cause one person to lose property and cause another person to obtain an economic benefit by inputting, altering, deleting, or suppressingcomputer data and/or interfering with the function of a computer system.
Article 11 – Attempt, aiding and abetting	Critical information infrastructure attacks may be used to attempt or to aid or abet crimes specified in the treaty.

Relevant Articles	Examples
Article 13 – Sanctions	The effects of critical information infrastructure attacks vary (they may differ in different countries for technical, cultural or other reasons), but governments normally care about them when they cause serious or widespread harm. A Party may foresee in its domestic law a sanction that is unsuitably lenient for critical information infrastructure attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. Parties may also consider aggravating circumstances, for example, if critical information infrastructure attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries.

3. T-CY statement

The above list of Articles related to critical information infrastructure attacks illustrates their multi-functional criminal use.

Therefore, the T-CY agrees that the different aspects of such attacks are covered by the Budapest Convention.

Guidance Note on new forms of Malware[36]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[37]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of new forms of malware.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[38] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to new forms of malware.

1. Relevant provisions of the Budapest Convention on Cybercrime (CETS 185)

There are many current forms of malware, which has been defined by the Organization for Economic Cooperation and Development as "a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners."[39] Commonly-known forms include worms, viruses, and trojans. Current forms of malware can steal data by copying it and sending it to another address; they can manipulate data; they can hinder the operation of computer systems, including those that control critical infrastructures; ransomware can delete, suppress or block access to data; and specially-tailored malware can target specified computer systems.

According to private and governmental sources, vast numbers of new forms of malware are developed and discovered every year. These new forms vary in their objectives. Like older forms, new forms of malware may steal money, or shut down water systems, or threaten users, and so on.

---

36. Adopted by the 9th Plenary of the T-CY (4-5 June 2013).
37. See the mandate of the T-CY (Article 46 Budapest Convention).
38. Paragraph 36 of the Explanatory Report.
39. www.oecd.org/internet/ieconomy/40724457.pdf.

The numbers and variety of forms of malware are so vast that it would not be possible to describe even currently-known forms in a criminal statute. The Cybercrime Convention deliberately avoids terms such as worms, viruses, and trojans. Because fashions in malware change, using such terms in a Convention would quickly make it obsolete and be counterproductive.

It is also not possible, of course, to describe future forms in a statute.

For these reasons, it is important to focus on the objectives and effects of the malware. These are already known and can be described in a statute.

Thus both current and future forms of malware are covered by the following sections of the Convention, depending on what the malware actually does. Each provision contains an intent standard ("without right," "with intent to defraud," etc) which should be taken into consideration when officials decide how to charge a crime.

2. T-CY interpretation of the criminalisation of new forms of malware

Relevant Articles	Examples
Article 2 – Illegal access	Malware can be used to access computer systems.
Article 3 – Illegal interception	Malware can be used to intercept non-public transmissions of computer data to, from, or within a computer system.
Article 4 – Data interference	Malware damages, deletes, deteriorates, alters or suppresses computer data.
Article 5 – System interference	Malware may hinder the functioning of a computer system
Article 6 – Misuse of devices	Malware is a device as defined in Article 6 (parties that take reservations to Article 6 must still criminalize the sale, distribution or making available of covered devices). This is because it will normally be designed or adapted primarily to commit the offences established by Articles 2 through 5. In addition, the article criminalizes the sale, procurement for use, import, distribution or other making available of computer passwords, access codes, or similar data by which computer systems may be accessed. These elements are frequently present in malware prosecutions.

Relevant Articles	Examples
Article 7 – Computer-related forgery	Malware may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Article 8 – Computer-related fraud	Malware may cause one person to lose property and cause another person to obtain an economic benefit by inputting, altering, deleting, or suppressing computer data and/or interfering with the function of a computer system.
Article 11 – Attempt, aiding and abetting	Malware may be used to attempt or to aid or abet several crimes specified in the treaty.
Article 13 – Sanctions	The effects of new forms of malware vary widely. Some malware is relatively trivial; other malware is dangerous to people, to critical infrastructures or in other ways. The effects may differ in different countries for technical, cultural or other reasons. A Party may foresee in its domestic law a sanction that is unsuitably lenient for malware attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. Parties may also consider aggravating circumstances, for example, if malware attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure.

3. T-CY statement

The above list of Articles related to all forms of malware illustrates the multi-functional criminal use of such attacks.

Therefore, the T-CY agrees that the different aspects of all forms of malware are covered by the Budapest Convention.

Guidance Note on Transborder access to data (Article 32)[40]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[41]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of transborder access to data under Article 32 Budapest Convention.[42]

Article 32b is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual assistance under limited circumstances. Parties are encouraged to make more effective use of all the international cooperation provisions of the Budapest Convention, including mutual assistance.

Overall, practices, procedures as well as conditions and safeguards vary considerably between different Parties. Concerns regarding procedural rights of suspects, privacy and the protection of personal data, the legal basis for access to data stored in foreign jurisdictions or "in the cloud" as well as national sovereignty persist and need to be addressed.

This Guidance Note is to facilitate implementation of the Budapest Convention by the Parties, to correct misunderstandings regarding transborder access under this treaty and to reassure third parties.

The Guidance Note will thus help Parties to take full advantage of the potential of the treaty with respect to transborder access to data.

---

40. Adopted by the 12th Plenary of the T-CY (2-3 December 2014)
41. See the mandate of the T-CY (Article 46 Budapest Convention).
42. The preparation of this Guidance Note represents follow up to the findings of the report on "Transborder access and jurisdiction" (T-CY(2012)3) adopted by the T-CY Plenary in December 2012. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

Article 32 Budapest Convention

Text of the provision:

> **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.

Extract of the Explanatory Report:

> 293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.
>
> 294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

T-CY interpretation of Article 32 Budapest Convention

With regard to Article 32a (transborder access to publicly available (open source) stored computer data) no specific issues have been raised and no further guidance by the T-CY is required at this point.

It is commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public.[43]

If a portion of a public website, service or similar is closed to the public, then it is not considered publicly available in the meaning of Article 32a.

Regarding Article 32b, typical situations may include:

- A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.[44]
- A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b.

Other situations are neither authorised nor precluded.[45]

With regard to Article 32b (transborder access with consent) the T-CY shares the following common understanding:

General considerations and safeguards

Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.[46]

---

43. Domestic law, however, may limit law enforcement access to or use of publicly available data.
44. Paragraph 294 Explanatory Report.
45. Paragraph 293 Explanatory Report. See also Article 39.3 Budapest Convention.
46. 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.

As pointed out above, it is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.[47]

The rights of individuals and the interests of third parties are to be taken into account when applying the measure.

Therefore, a searching Party may consider notifying relevant authorities of the searched Party.

(Footnote 46– Continued)

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.

47. 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.

On the notion of "transborder" and "location"

Transborder access means to "unilaterally access computer data stored in another Party without seeking mutual assistance".[48]

The measure can be applied between the Parties.

Article 32b refers to "stored computer data located in another Party". This implies that Article 32b may be made use of if it is known where the data are located.

Article 32b would not cover situations where the data are not stored in another Party or where it is uncertain where the data are located. A party may not use article 32b to obtain disclosure of data that is stored domestically.

Article 32b "neither authorise[s], nor preclude[s]" other situations. Thus, in situations where it is unknown whether, or not certain that, data are stored in another Party, Parties may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations.

On the notion of "access without the authorisation of another Party"

Article 32b does not require mutual assistance, and the Budapest Convention does not require a notification of the other Party. At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

On the notion of "consent"

Article 32b stipulates that consent must be lawful and voluntary which means that the person providing access or agreeing to disclose data may not be forced or deceived.[49]

Subject to domestic legislation, a minor may not be able to give consent, or persons because of mental or other conditions may also not be able to consent.

In most Parties, cooperation in a criminal investigation would require explicit consent. For example, general agreement by a person to terms and conditions of an online service used might not constitute explicit consent even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse.

48. Paragraph 293 Explanatory Report to the Budapest Convention.
49. In some countries, consenting to avoid or reduce criminal charges or a prison sentence also constitutes lawful and voluntary consent.

On the applicable law

In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b.

It is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.

On the person who can provide access or disclose data

As to "who" is the person who is "lawfully authorised" to disclose the data, this may vary depending on the circumstances, laws and regulations applicable.

For example, it may be a physical individual person, providing access to his email account or other data that he stored abroad.[50]

It may also be a legal person.

Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent. Of course, law enforcement agencies may be able to procure data transnationally by other methods, such as mutual legal assistance or procedures for emergency situations.

Domestic lawful requests versus Article 32b

Article 32b is not relevant to domestic production orders or similar lawful requests internal to a Party.

On the location of the person consenting to provide access or disclose data

The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party.

However, multiple situations are possible. It is conceivable that the physical or legal person is located in the territory of the requesting law enforcement authority when agreeing to disclose or actually providing access, or only when agreeing to disclose but not when providing access, or the person is located in the country where the data is stored when agreeing to disclose and/or providing access. The person may also be physically located in a third country when agreeing to cooperate or when actually providing access. If the

50. See the example given in Paragraph 294 Explanatory Report.

person is a legal person (such as a private sector entity), this person may be represented in the territory of the requesting law enforcement authority, the territory hosting the data or even a third country at the same time.

It should be taken into account that many Parties would object – and some even consider it a criminal offence – if a person who is physically in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation.

T-CY Statement

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of Article 32.

Guidance Note Spam[51]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[52]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of spam. The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[53] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to spam.

Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

Spam is often defined as unsolicited bulk email, where a message is sent to a significant number of email addresses, where the recipient's personal identity is irrelevant because the message is equally targeted at many other recipients without distinction.

There are separate issues relating to:

- the content of spam,
- the action of sending spam, and
- the mechanism used to transmit spam.

The content of spam may or may not be illegal, and where the content is illegal (such as offering fake medicines or fraudulent financial offerings) the offence may fall under the relevant national legislation for those offences. The action of transmitting spam (including bulk transmission of non-objectionable content) may be a civil or criminal offence in jurisdictions.

---

51. Adopted by the 12th Plenary of the T-CY (2-3 December 2014).
52. See the mandate of the T-CY (Article 46 Budapest Convention).
53. Paragraph 36 of the Explanatory Report.

The Convention does not cover spam the contents of which is not illegal and does not cause system interference, but may be a nuisance to end-users.

The tools used to transmit spam may be illegal under the Budapest Convention, and spam may be associated with other offences not listed in the matrix below (see, for example, Article 7).

As with other guidance notes, each provision contains an intent standard ("without right", "with intent to defraud," etc). In some spam cases this intent may be difficult to prove.

T-CY interpretation of provisions addressing spam

Relevant Articles	Examples
Article 2 – Illegal access	Spam may contain malware that may access or enable access to a computer system.
Article 3 – Illegal interception	Spam may contain malware that may illegally intercept or enable the illegal interception of transmissions of computer data.
Article 4 – Data interference	Spam may contain malware that may damage, delete, deteriorate, alter or suppress computer data.
Article 5 – System interference	The transmission of spam may seriously hinder the functioning of computer systems. Spam may contain malware that seriously hinders the functioning of computer systems.
Article 6 – Misuse of devices	Devices as defined by Article 6 may be used for the transmission of spam. Spam may contain devices as defined by Article 6.
Article 8 – Computer-related fraud	Spam may be used as a device for input, alteration, deletion or suppression of computer data or interference with the functioning of a computer system for procuring illegal economic benefit.
Article 10 – Offences related to infringements of copyright	Spam may be used for advertising the sale of fake goods, including software and other items protected by copyright.

Relevant Articles	Examples
Article 11 – Attempt, aiding and abetting	Spam and the transmission of spam may be used to attempt or to aid or abet several crimes specified in the treaty (such as Article 7 on computer-related forgery or Article 8 on computer-related fraud).
Article 13 – Sanctions	Spam may serve multiple criminal purposes some of which have serious impact on individuals, or public or private sector institutions. Even if a Party does not criminalise spam *per se,* it should criminalise spam-related conduct such as the above offences, and it may consider aggravated circumstances. Parties should ensure, pursuant to Article 13, that criminal offences related to spam "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions.

T-CY statement

The above list of Articles illustrates the multi-functional criminal use of spam and spam-related offences.

Therefore, the T-CY agrees that these aspects of spam are covered by the Budapest Convention.

Guidance Note on Production orders for subscriber information (Article 18 Budapest Convention)[54]

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[55]

While not binding, Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note[56] addresses the question of production orders for subscriber information under Article 18, that is, situations in which:

- a person ordered to submit specified computer data is present in the territory of a Party (Article 18.1.a);57
- a service provider ordered to submit subscriber information is offering its services in the territory of the Party without necessarily being located in the territory (Article 18.1.b).

A Guidance Note on these aspects of Article 18 is relevant given that:

- subscriber information is the most often sought data in criminal investigations;
- Article 18 is a domestic power;
- the growth of cloud computing and remote data storage has raised a number of challenges for competent authorities seeking access to specified computer data – and, in particular, subscriber information – to further criminal investigations and prosecutions;
- currently, practices and procedures, as well as conditions and safeguards for access to subscriber information vary considerably among Parties to the Convention;
- concerns regarding privacy and the protection of personal data, the legal basis for jurisdiction pertaining to services offered in the territory of a Party without the service provider being established in that territory, as

54. Adopted by the T-CY following the 16th Plenary by written procedure (28 February 2017)
55. See the mandate of the T-CY (Article 46 Budapest Convention).
56. This Guidance Note is based on the work of the T-CY Cloud Evidence Group.
57. It is important to recall that Article 18.1.a of the Budapest Convention is not limited to subscriber information but concerns any type of specified computer data. This Guidance Note, however, addresses the production of subscriber information only.

well as access to data stored in foreign jurisdictions or in unknown or multiple locations "within the cloud" need to be addressed.

The service and enforceability of domestic production orders against providers established outside the territory of a Party raises further issues which cannot be fully addressed in a Guidance Note. Some Parties may require that subscriber information be requested through mutual legal assistance.

Article 18 is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14 Budapest Convention. Orders are thus to be issued in specific cases with regard to specified subscribers.

Article 18 Budapest Convention

Text of the provision

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.

Extract from the Explanatory Report:

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

> Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.[58]

What is "subscriber information?"

The term "subscriber information" is defined in Article 18.3 of the Budapest Convention:

> 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
>
> a the type of communication service used, the technical provisions taken thereto and the period of service;
>
> b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
>
> c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Paragraph 177 Explanatory Report furthermore notes:

> 177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

Obtaining subscriber information may represent a lesser interference with the rights of individuals than obtaining traffic data or content data.

---

58. Paragraph 173 Explanatory Report.

What is a "service provider?"

The Budapest Convention on Cybercrime applies a broad concept of "service provider" which is defined in Article 1.c of the Budapest Convention.

For the purposes of this Convention:

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.

Article 18.1.b is to be applied with respect to any service provider offering its services in the territory of the Party.[59]

T-CY interpretation of Article 18 Budapest Convention with respect to subscriber information

The scope of Article 18.1.a

- The scope is broad: a "person" (which may include a "service provider") that is present in the Party's territory.
- With respect to computer data, the scope is broad but not indiscriminate: any "specified" computer data[2] (hence Article 18.1.a is not restricted to "subscriber information" and covers all types of computer data).
- The specified computer data is in that person's possession or, if the person has no physical possession, that person freely controls the computer data to be submitted under Article 18.1.a from within the Party's territory.
- The specified computer data is stored in a computer system or a computer-data storage medium.
- The production order is issued and enforceable by the competent authorities in the Party in which the order is sought and granted.

The scope of Article 18.1.b

The scope of Article 18.1.b is narrower than that of Article 18.1.a:

59. European Union instruments distinguish between providers of electronic communication services and of Internet society services. The concept of "service provider" of Article 1.c Budapest Convention encompasses both.

- Subsection b is restricted to a "service provider".[60]
- The service provider to which the order is issued is not necessarily present, but offers its services in the territory of the Party.
- It is restricted to "subscriber information."
- The subscriber information relates to such services and is in that service provider's possession or control.

In contrast to Article 18.1.a which is restricted in scope of application to "persons present in the territory of the Party", 18.1.b is silent on the issue of the location of the service provider. Parties could apply the provision in circumstances in which the service provider offering its services in the territory of the Party is neither legally nor physically present in the territory.

Jurisdiction

Article 18.1.b is restricted to circumstances in which the criminal justice authority issuing the production order has jurisdiction over the offence.

This may include situations in which the subscriber is or was resident or present in that territory when the crime was committed.

The present interpretation of Article 18 is without prejudice to broader or additional powers under the domestic law of Parties.

Agreement to this Guidance Note does not entail consent to the extraterritorial service or enforcement of a domestic production order issued by another State nor creates new obligations or relationships between the Parties.

What are the characteristics of a "production order?"

A "production order" under Article 18 is a domestic measure and is to be provided for under domestic criminal law. A "production order" is constrained by the adjudicative and enforcement jurisdiction of the Party in which the order is granted.

Production orders under Article 18 refer:

to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some

60. The "person" is a broader concept than "a service provider", although a "service provider" can be "a person".

service providers, for example, do not keep records regarding the subscribers to their services.[61]

The Explanatory Report[62] to the Budapest Convention refers to production orders as a flexible measure which is less intrusive than search or seizure or other coercive powers and further states that:

the implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

What effect does the location of the data have?

The storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention as long as such data is in the possession or control of the service provider. The Explanatory Report states with respect to:

- Article 18.1.a that "the term "possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory."[63]
- Article 18.1.b that "the term "possession or control' refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company)."[64]

Regarding Article 18.1.b, a situation may include a service provider that has its headquarters in one jurisdiction, but stores the data in another jurisdiction. Data may also be mirrored in several jurisdictions or move between jurisdictions according to service provider discretion and without the knowledge or control of the subscriber. Legal regimes increasingly recognise that, both in the criminal justice sphere and in the privacy and data protection sphere, the location of the data is not the determining factor for establishing jurisdiction.

61. Paragraph 172 Explanatory Report.
62. Paragraph 171 Explanatory Report.
63. Paragraph 173 Explanatory Report. A "person" in Article 18.1.a Budapest Convention may be a physical or legal person, including a service provider.
64. Paragraph 173 Explanatory Report.

What is "offering its services in the territory of a Party?"

The growth of cloud computing has raised questions as to when a service provider is considered to be offering its services in the territory of the Party and thus may be issued a domestic production order for subscriber information. This has led to a range of interpretations across multiple jurisdictions by courts in both civil and criminal cases.

With regard to Article 18.1.b, Parties could consider that a service provider is "offering its services in the territory of the Party", when:

- the service provider enables persons in the territory of the Party to subscribe to its services[65] (and does not, for example, block access to such services);

and

- the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.

The sole fact that a service provider makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country. Therefore, the requirement that the subscriber information to be produced is relating to services of a provider offered in the territory of the Party may be considered to be met even if those services are provided via a country code top-level domain name referring to another jurisdiction.

General considerations and safeguards

The Parties to the Convention are expected to form a community of trust that respects Article 15 Budapest Convention.

> **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

65. Note Paragraph 183 Explanatory Report: "The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services."

provide for the adequate protection of human rights and liberties, including rights against 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.

Applying Article 18 with respect to subscriber information

The production of subscriber information under Article 18 Budapest Convention could, therefore, be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers:

<table>
<tr><td colspan="3">IF
The criminal justice authority has jurisdiction over the offence;</td></tr>
<tr><td colspan="3">AND IF
the service provider is in possession or control of the subscriber information;</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td>Article 18.1.a
The person (service provider) is in the territory of the Party.</td><td>OR</td><td>Article 18.1.b
A Party considers that a service provider is “offering its services in the territory of the Party” when, for example:
– the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);
and
– the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td></td><td></td><td>– the subscriber information to be submitted is relating to services of a provider offered in the territory of the Party.</td></tr>
</table>

T-CY statement

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of Article 18 Budapest Convention with respect to the production of subscriber information.

Guidance Note on Terrorism[66]

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[67]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses how different Articles of the Convention could apply to terrorism.

Many countries are Parties to numerous treaties, and subject to UN Security Council Resolutions, that require criminalization of different forms of terrorism, facilitation of terrorism, support for terrorism, and preparatory acts. In terrorism cases, countries often rely on offenses that derive from those topic-specific treaties, as well as additional offenses in national legislation.

The Budapest Convention is not a treaty that is focused specifically on terrorism. However, the substantive crimes in the Convention may be carried out as acts of terrorism, to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.

The scope and limits are defined by Articles 14.2 and 25.1 Budapest Convention:

> **Article 14.2**
>
> 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.

66. Adopted by the T-CY following the 16th Plenary by written procedure (28 February 2017).
67. See the mandate of the T-CY (Article 46 Budapest Convention).

Article 25.1

"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."

See also Articles 23 and 27.1 Budapest Convention as well as other Guidance Notes, such as the Guidance Notes on critical infrastructure attacks or distributed denial of service attacks.

Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

Procedural provisions

The Convention's procedural powers (Articles 14-21) may be used in a specific criminal investigation or proceeding in any type of case, as Article 14 provides.

In fact, the specific procedural measures can be very useful, for example in terrorism cases, if a computer system was used to commit or facilitate the offence or if the evidence of that offence is stored in electronic form or if a suspect can be identified through subscriber information, including an Internet Protocol address. Thus, in terrorism cases, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

International mutual legal assistance provisions

The Convention's international cooperation powers (Articles 23-35) are of similar breadth.

Thus, Parties must make available expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools, as well as other international cooperation provisions, in order to cooperate with other Parties in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

Substantive criminal law provisions

Finally, as noted above, terrorists and terrorist groups may carry out acts criminalized by the Convention as part of achieving their goals.

Relevant Articles	Examples
Article 2 – Illegal access	A computer system may be illegally accessed to obtain personally identifiable information (e.g. information about government employees to target them for attack).
Article 3 – Illegal interception	Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain information about a person's location (e.g. to target that person).
Article 4 – Data interference	Computer data may be damaged, deleted, deteriorated, altered, or suppressed (e.g. a hospital's medical records can be altered to be dangerously incorrect, or interference with an air traffic control system can affect flight safety).
Article 5 – System interference	The functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure).
Article 6 – Misuse of devices	The sale, procurement for use, import, distribution or other acts making available of computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate a terrorist attack (e.g. it can lead to damage to a country's electrical power grid).
Article 7 – Computer-related forgery	Computer data (for example the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Article 8 – Computer-related fraud	Computer data may be input, altered, deleted, or suppressed, and/or the function of a computer system may be interfered with, causing other persons to lose property (for example, an attack on a country's banking system can cause loss of property to a number of victims).
Article 11 – Attempt, aiding and abetting	Crimes specified in the treaty may be attempted, aided or abetted in furtherance of terrorism.
Article 12 – Corporate liability	Crimes covered by Articles 2-11 of the Convention in furtherance of terrorism may be carried out by legal persons who would be liable under Article 12.

Relevant Articles	Examples
Article 13 – Sanctions	Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against systems that are crucial to daily life, for example public transport, banking systems or hospital infrastructure. The effects may differ in different countries, depending also on their degree of interconnectedness and their dependence on such systems. A Party may provide in its domestic law a sanction that is unsuitably lenient for terrorism-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". Parties may also consider aggravating circumstances, for example if such acts affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure.

Other crimes covered by the Convention but not mentioned specifically above, including the production of child exploitation materials or trafficking in stolen intellectual property, may also be carried out in connection with terrorism.

For Parties to the Budapest Convention which are also Parties to the Additional Protocol on Xenophobia and Racism Committed Through Computer Systems (ETS 189)[68], two articles of the Protocol are relevant as these may relate to radicalisation and violent extremism which may lead to terrorism. These are Article 4 of the Protocol covering racist and xenophobic motivated threat and Article 6 covering denial, gross minimisation, approval or justification of genocide or crimes against humanity.

T-CY statement

The T-CY agrees that the substantive crimes in the Convention may also be acts of terrorism as defined in applicable law.

68. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

The substantive crimes in the Convention may be carried out to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

The procedural and mutual legal assistance tools in the Convention may be used to investigate terrorism, its facilitation, support for it, or preparatory acts.

Guidance Note on Aspects of election interference by means of computer systems covered by the Budapest Convention[69]

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[70]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

Interference with elections through malicious cyber activities against computers and data used in elections and election campaigns undermines free, fair and clean elections and trust in democracy. Disinformation operations, as experienced in particular since 2016, may make use of malicious cyber activities and may have the same effect. Domestic election procedures may need to be adapted to the realities of the information society, and computer systems used in elections and related campaigns need to be made more secure.

In this context, greater efforts need to be undertaken to prosecute such interference where it constitutes a criminal offence: an effective criminal justice response may deter election interference and reassure the electorate with regard to the use of information and communication technologies in elections.

The present Note addresses how Articles of the Convention may apply to aspects of election interference by means of computer systems.

The substantive criminal offences of the Convention may be carried out as acts of election interference or as preparatory acts facilitating such interference.

In addition, the domestic procedural and international mutual legal assistance tools of the Convention are available for investigations and prosecutions related to election interference. The scope and limits of procedural powers and tools for international cooperation are defined by Articles 14.2 and 25.1 Budapest Convention:

> Article 14.2
>
> 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:

69. Adopted by T-CY 21 (8 July 2019).
70. See the mandate of the T-CY (Article 46 Budapest Convention).

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.

Article 25.1

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.

The procedural powers of the Convention are subject to the conditions and safeguards of Article 15.

Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

Procedural provisions

The Convention's procedural powers (Articles 14-21) may be used in a specific criminal investigation or proceeding in any type of election interference, as Article 14 provides.

The specific procedural measures can be very useful in criminal investigations of election interference. For example, in cases of election interference, a computer system may be used to commit or facilitate an offence, the evidence of that offence may be stored in electronic form, or a suspect may be identifiable through subscriber information, including an Internet Protocol address. Similarly, illegal political financing may be traceable via preserved email, voice communications between conspirators may be captured pursuant to properly authorised interception, and misuse of data may be illustrated by electronic trails.

Thus, in criminal investigations of election interference, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence needed for the investigation and prosecution of such offences relating to election interference.

International mutual legal assistance provisions

The Convention's international cooperation powers (Articles 23-35) are of similar breadth and may assist Parties in investigations of election interference.

Thus, Parties shall make available expedited preservation of stored computer data, production orders, search and seizure of stored computer data, as well as other international cooperation provisions.

Substantive criminal law provisions

Finally, as noted above, election interference may involve the following types of conduct, when done without right, as criminalised by the Convention on Cybercrime. The T-CY emphasises that the examples below are merely examples – that is, since election interference is a developing phenomenon, it may appear in many forms not listed below. However, the T-CY expects that the Convention on Cybercrime is sufficiently flexible to address them.

Relevant Articles	Examples
Article 2 – Illegal access	A computer system may be illegally accessed to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters.
Article 3 – Illegal interception	Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters.
Article 4 – Data interference	Computer data may be damaged, deleted, deteriorated, altered, or suppressed to modify websites, to alter voter databases, or to manipulate results of votes such as by tampering with voting machines.
Article 5 – System interference	The functioning of computer systems used in elections or campaigns may be hindered to interfere with campaign messaging, hinder voter registration, disable the casting of votes or prevent the counting of votes through denial of service attacks, malware or other means.
Article 6 – Misuse of devices	The sale, procurement for use, import, distribution or other acts making available computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate election interference such as the theft of sensitive data from political candidates, parties or campaigns.

Article 7 – Computer-related forgery	Computer data (for example the data used in voter databases) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. For example, some countries require election campaigns to make public financial disclosures. Forgery of computer data could create the impression of incorrect disclosures or hide questionable sources of campaign funds.
Article 11 – Attempt, aiding and abetting	Crimes specified in the treaty may be attempted, aided or abetted in furtherance of election interference.
Article 12 – Corporate liability	Crimes covered by Articles 2-11 of the Convention in furtherance of election interference may be carried out by legal persons that would be liable under Article 12.
Article 13 – Sanctions	Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against fundamentals of political life such as elections. Criminal actions and their effects may differ in different countries, but election interference may undermine trust in democratic processes, change the outcome of an election, require the expense and upheaval of a second election, or cause physical violence between election partisans and communities. A Party may provide in its domestic law a sanction that is unsuitably lenient for election-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". Parties may also consider aggravating circumstances, for example, if such acts affect an election significantly or cause deaths or physical injuries or significant material damage.

T-CY statement

The T-CY agrees that the substantive offences in the Convention may also be acts of election interference as defined in applicable law, that is, offences against free, fair and clean elections.

The substantive crimes in the Convention may be carried out to facilitate, participate in or prepare acts of election interference.

The procedural and mutual legal assistance tools in the Convention may be used to investigate election interference, its facilitation, participation in it, or preparatory acts.

Guidance Note on Aspects of ransomware covered by the Budapest Convention

Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Convention on Cybercrime, also in the light of legal, policy and technological developments.[71]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

Offenders, for decades, have committed different forms of cybercrime in order to extort ransoms from organisations and individuals. For example, the theft and subsequent threat of public disclosure of personal data or other sensitive information to coerce payment of ransom is still prevalent. However, over the past decade more complex forms of ransomware and related offences have emerged. These entail the encryption of computer data or systems, thus locking out users, followed by requests for ransom against the (promise of) access to be restored. Offenders may also threaten to release sensitive or personal information, in an attempt to more effectively extract payments from victims.

Such ransomware offences are possible because of technology permitting:

- strong encryption of victims' computer data or systems;
- use of communication systems that are difficult to trace in order to send requests for ransom payments as well as decryption tools;
- payment of ransom in a manner that is difficult to trace such as through virtual currencies that are easier to obfuscate than traditional fiat currencies.

The "WannaCry" and "NotPetya" attacks of 2016/2017 affected computers and attracted major attention worldwide. The COVID-19 pandemic from 2020 onwards led to a greater reliance of societies on information and communication technology, increasing opportunities for exploitation for criminal purposes. This contributed to a further surge in ransomware offences. Attacks against computer systems of hospitals have reportedly led to the death of patients. Further, ransomware offences against critical infrastructure caused a national emergency to be declared in Costa Rica in April 2022. The use of ransomware is now considered a serious form of cybercrime that is affecting essential interests of individuals, businesses, societies and governments.

71. See the mandate of the T-CY (Article 46 Budapest Convention).

The T-CY, therefore, at its 26th plenary (10-11 May 2022), decided to prepare a Guidance Note to show how aspects of ransomware offences are criminalised under the substantive criminal law provisions of the Convention on Cybercrime and how the procedural powers and provisions on international co-operation of this treaty may be used to investigate, prosecute and co-operate against ransomware offences.

The present Guidance Notes also makes reference to the Second Additional Protocol to the Convention on Cybercrime (CETS 224) that will provide additional tools for "enhanced co-operation and disclosure of electronic evidence" to Parties to this Protocol once it is in force.

Previous T-CY Guidance Notes on malware, botnets, identify theft and critical infrastructure attacks remain relevant with regard to ransomware offences as well.

Ransomware offences

Ransomware is a type of malware that is designed to deny a user access to their computer data or computer system by encrypting such data or systems. The user targeted is then requested to pay a ransom for (the promise of) access to the data or system to be restored.

Ransomware offences typically involve:

1. Preparatory acts, including:
   - the production, sale, procurement or otherwise making available of ransomware, that is, of a "device" in the meaning of Article 6 of the Convention on Cybercrime;
   - the production, sale, procurement or otherwise making available of other devices in the meaning of Article 6 that are used in the preparation of ransomware offences, such as malware to gain unauthorized access to victim systems, or botnets to distribute ransomware;
   - obtaining mailing lists or other relevant information on targets. Some of such preparatory acts may themselves be offences or may be considered aiding or abetting ransomware offences, such as exfiltration of databases using keyloggers, use of botnets, or identity theft.[72]

72. See relevant Guidance Notes (coe.int)

2. The distribution or installation of ransomware, including:

- through emails with attachments containing the malware or targeting users of messaging applications with links embedded in messages. Enticing users to access such attachments or links – and thus to install the malware – may be further facilitated through social engineering or other techniques of identity theft;
- through remote access to a computer system.

3. Encryption of the computer system, or parts of it, or data through the ransomware and thus preventing the user from accessing or otherwise making use of the data or system.

4. Requesting, obtaining and transferring the ransom payment, including:

- requesting the ransom in exchange for (the promise of) restoring access to the data and/or system which amounts to extortion or blackmail but possibly also other offences;
- communication between the offender and the target through means of communication that are difficult to trace, including use of TOR. Decryption tools may also be communicated in this manner;
- obtaining the ransom in a manner that makes it difficult to trace, typically in the form of cryptocurrency, often followed by the laundering of the proceeds to further hide the identity of the perpetrator and the proceeds.

Since 2021, the market for ransomware is increasingly organised and professional, offering a business model often referred to as ransomware-as-a-service (or RaaS) to commit ransomware offences. This business model has led to cyber criminals involving independent services to negotiate payments, assist victims with making payments, and some services offering a 24/7 help centre to expedite ransom payments and to assist in the restoration of encrypted systems or data.

Relevant provisions of the Convention on Cybercrime (ETS 185)

Criminalisation of offences related to ransomware

Under the Convention on Cybercrime, each Party shall adopt legislative and other measures as may be necessary to establish certain criminal offences under its domestic law, when committed intentionally and without right. The following articles and corresponding offences under the domestic laws of Parties implementing the Convention would be relevant for investigations and criminal proceedings regarding ransomware offenses.

Relevant Articles	Examples
Article 2 – Illegal access	Ransomware offences involve illegal access to a computer system of a victim and thus a criminal offence according to Article 2.
Article 3 – Illegal interception	Ransomware variants may include the capability to intercept non-public transmissions of computer data to, from or within a computer system. The procurement of information on targets or of access credentials may also involve the offence of illegal interception.
Article 4 – Data interference	Ransomware is specifically designed for the purpose of interfering with computer data and its use is thus a criminal offence according to Article 4.
Article 5 – System interference	Ransomware may be designed for the purpose of interfering with the functioning of a computer system and its use is thus a criminal offence according to Article 5.
Article 6 – Misuse of devices	Ransomware is malware and thus a device "designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5". Thus, the "production, sale, procurement for use, import, distribution or otherwise making available" of ransomware is a criminal offence according to Article 6.
Article 7 – Computer-related forgery	In order to gain illegal access to victims' systems, ransomware actors often use phishing and other social engineering techniques – which in certain cases may constitute computer-related forgery – that is creating inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.
Article 8 – Computer-related fraud	Ransomware offences cause the loss of property by interfering with computer data and/or the functioning of a computer system with fraudulent or other dishonest intent of procuring, without right, an economic benefit.
Article 11 – Attempt, aiding and abetting	Offences provided for in the treaty may be attempted, aided or abetted in furtherance of ransomware-related offences. Different persons may be involved, for example, in the production, procurement or otherwise making available of ransomware, or in the procurement of information on targets.

Relevant Articles	Examples
Article 12 – Corporate liability	Ransomware offences covered by Articles 2-11 of the Convention as described above may be carried out by legal persons that would be liable according to Article 12.
Article 13 – Sanctions	Offences related to ransomware that are crimes covered by the Convention may pose a significant threat to individuals and to society, especially when the crimes are directed against critical information infrastructure and cause significant risk to the life or safety of any natural person. Parties should therefore ensure, pursuant to Article 13, that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". This includes ensuring that, under its domestic law, the available sanctions are appropriate given the threat posed by ransomware and take into consideration the full range of criminal liability, including on the basis of attempting, aiding, and abetting criminal activity. Parties may also consider more severe penalties when aggravating circumstances are present, for example, if such acts affect the functioning of critical infrastructure significantly or cause death or physical injury of a natural person or significant material damage.

Therefore, ransomware offences may comprise conduct that is to be criminalised according to Articles 2 to 8 as well as under Article 11 (attempt, aiding or abetting), and that may also entail the liability of legal persons under Article 12 of the Convention on Cybercrime.

Ransomware activities may comprise a wide range of other offences under domestic criminal law.

Procedural provisions

Under the Convention on Cybercrime "[e]ach Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to" undertake certain procedural measures to investigate the offences according to articles 2-11 of the Convention and to collect evidence in electronic form (see Article 14 of the Convention). These may also be used for investigations and criminal proceedings related to ransomware offences.

Relevant Articles	Examples
Article 14 – Scope of procedural provisions	The procedural powers of the Convention (Articles 16-21) may be used in a specific criminal investigation or proceeding not only in respect to the above offences under the Convention but also in respect to the collection of evidence in electronic form of any other offence related to ransomware as defined under the domestic law of a Party.
Article 15 – Conditions and safeguards	These conditions and safeguards also apply to criminal investigations and proceedings related to ransomware offences.
Article 16 – Expedited preservation of stored computer data	This power may be used to expeditiously preserve stored computer related to ransomware offences, including, for example, data on the source or path of ransomware distribution or of communications requesting ransom or providing decryption tools if applicable. This power may also be used to order the preservation of other data related to ransomware offences, such as communications between suspects or data stored by suspects that may be evidence of such offences.
Article 17 – Expedited preservation and partial disclosure of traffic data	This power may be used to expeditiously obtain a sufficient amount of traffic data to identify other service providers and the path through which communications related to ransomware offences were transmitted.
Article 18 – Production order	Production orders according to Article 18 may be used to order a person to produce stored computer data related to ransomware offences. This may include service providers, financial institutions including virtual assets service providers and platforms, and other legal or natural persons. These orders are vital to obtaining, for example, subscriber information from providers related to accounts and infrastructure associated with ransomware.
Article 19 – Search and seizure of stored computer data	Search and seizure provisions according to Article 19 may be used to search and seize stored computer data related to ransomware offences.
Article 20 – Real-time collection of traffic data	Powers according to Article 20 may be used for the real-time collection of traffic data related to ransomware offences.
Article 21– Interception of content data	Powers according to Article 21 may be used for the interception of certain content data related to ransomware offences, such as, for example, communications between suspects.

Thus, in criminal investigations or proceedings related to ransomware offences, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence.

International co-operation provisions

Relevant Articles	Examples
General principles and procedures relating to international co-operation of Articles 23 – 28	The general principles and procedures for international co-operation of Articles 23 to 28 of the Convention – that is on extradition, mutual assistance and others – are also applicable to offences related to ransomware. Article 26 may be particularly useful in that a Party possessing valuable information on ransomware offences obtained through its own investigations may, within the limits of its domestic law, forward such information to the other Party without a prior request (see paragraph 260 of the Explanatory Report to the Convention on Cybercrime). According to Article 23 and Article 25.1, Parties to the Convention are required to cooperate with each other, in accordance with the provisions of Articles 23-28, "to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data" and for "the collection of evidence in electronic form of a criminal offence."
Specific provisions on international co-operation of Articles 29 – 35.	The specific provisions of Chapter III of the Convention are available for international co-operation and collection of evidence related to ransomware offences: – Article 29 – Expedited preservation of stored computer data – Article 30 – Expedited disclosure of preserved traffic data – Article 31 – Mutual assistance regarding accessing of stored computer data – Article 32 – Trans-border access to stored computer data with consent or where publicly available – Article 33 – Mutual assistance in the real-time collection of traffic data – Article 34 – Mutual assistance regarding the interception of content data – Article 35 – 24/7 network

Given that ransomware offences typically involve offenders, targets and victims, service providers, financial institutions or computer systems in multiple jurisdictions, effective use of these international co-operation provisions is particularly important.

The Second Additional Protocol to the Convention on Cybercrime (CETS 224)

On 12 May 2022, the Second Additional Protocol to the Convention on Cybercrime (CETS 224) was opened for signature. Once in force, this instrument will provide Parties to it with additional tools for "enhanced co-operation and disclosure of electronic evidence". These will be relevant, and in some instances highly relevant, to criminal investigations and proceedings related to ransomware offences, and include:

- Article 6 – Request for domain name registration information directly to an entity in another Party providing domain name registration services;
- Article 7 – Disclosure of subscriber information through direct co-operation with a service provider in another Party;
- Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data;
- Article 9 – Expedited disclosure of stored computer data in an emergency;
- Article 10 – Emergency mutual assistance;
- Article 11 – Video conferencing;
- Article 12 – Joint investigation teams and joint investigations.

The scope of application of this Protocol is again broad in that it shall be applied not only to criminal offences related to computer systems and data but also to the collection of evidence in electronic form of any criminal offence (see Article 2.1.a).

The conditions and safeguards of Article 13 ensure that the establishment, implementation, and application of the powers and procedures provided for in the Protocol are subject to conditions and safeguards provided for by each Party's domestic law, which must provide for the adequate protection of human rights and liberties. Additionally, given that many Parties to the Protocol may be required, in order to meet their constitutional or international obligations, to ensure the protection of personal data, Article 14 provides for data protection safeguards to permit Parties to meet such requirements

and ensures that personal data can be transferred when making use of these expedited forms of co-operation.

T-CY statement

The T-CY agrees that:

- offences related to ransomware attacks may comprise conduct that is to be criminalised according to Articles 2 to 8 as well as under Article 11 (attempt, aiding or abetting), and that may entail the liability of legal persons under Article 12 of the Convention on Cybercrime;
- the procedural measures and international-cooperation tools of the Convention may be used to investigate and prosecute ransomware attacks and related offences, as well as their facilitation, participation in such offenses, or preparatory acts;
- the Second Additional Protocol to the Convention on Cybercrime, once in force, will provide its Parties further tools for enhanced co-operation and disclosure of electronic evidence related to ransomware attacks.

PREMS 001323

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE