Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 15316 rev
02 September 2021

Draft second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

Request for an opinion
Committee of Ministers

Contents **Page**

Letter from the Secretary to the Committee of Ministers ad interim to the Secretary General of the Parliamentary Assembly (Strasbourg, 17 May 2021) 2

Appendix 1 – Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence 3

Appendix 2 – Explanatory report 20

Letter from the Secretary to the Committee of Ministers ad interim to the Secretary General of the Parliamentary Assembly (Strasbourg, 17 May 2021)

Please find enclosed the Draft Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CM(2021)57-rev2), which the Ministers' Deputies agreed to transmit to the Parliamentary Assembly for opinion at their 1404th meeting (12 May 2021), as well as its draft Explanatory Report (CM(2021)57-addrev).

Signed

Leyla Kayacik, Secretary to the Committee of Ministers ad interim

Appendix 1 – Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

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

1. 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. an "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 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 relates 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 the 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 relates 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 has 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 has 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, 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 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. the 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 the 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, paragraph 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, specify that this Protocol shall not apply to one or more territories specified in the Party's declaration under Article 38, paragraphs 1 and 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 Articles 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 Articles 7, paragraphs 2.b and 8; Article 8, paragraph 11; Article 9, paragraphs 1.b and 5; Article 10, paragraph 9.b; 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 the declaration(s), notifications or communications identified in Article 7, paragraphs 5.a and e; 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 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.

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

Done at xx, this xx day of xx 20xx, 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 Parties and Signatories to the Convention, and to any State which has been invited to accede to the Convention.

Appendix 2 – Explanatory report

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 [xxx] meeting ([day month year]) of the Minister's Deputies, and the Protocol was opened for signature in [place] on [day month year] [on the issue of the [conference] and [ ]]. 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 extra-ordinary 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; as well as 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 aimed principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime (2) 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 (3) setting up a fast and effective regime of international.

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) (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 (a) the common standards of the Convention in the area of cybercrime, coupled with (b) a robust mechanism for ongoing Party engagement through the T-CY, and (c) 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 "exchang[e] 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 and data flows ("Transborder Group"). In December 2014, the T-CY had already 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 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 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 ten 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 the Protocol and to develop innovative solutions.

17. The European Union Commission participated in this work on behalf of the State 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, those 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, industry and with data protection experts: in conjunction with the Octopus Conference on 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 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 Automated 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 were 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 and Cloud Evidence groups 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 the Protocol, mutual assistance requests were the primary method to obtain electronic evidence of a criminal offense 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 email 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.

– 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 in 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 bi- and multi-lateral agreements. However, such mechanisms are not universally available among Parties to the Convention, and the 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. Further, 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 party 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 (ETS No. 223) was opened for signature during the drafting of this Protocol on October 2018. It should be also noted that the drafting process of this Protocol included Parties not subject, at the time, to Council of Europe instruments on data protection nor 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 the 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 timeframe 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. The 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.

The Protocol

26. As noted 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, the Protocol relates to specific criminal investigations or proceedings, and 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 the 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 the 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 for Chapter II, (2) procedures for enhancing direct co-operation with service providers and entities providing domain name registration services 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 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 the Protocol

Chapter I – Common provisions

Article 1 – Purpose

32. 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 thereto that are also Party 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-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 2.1.b states that as between Parties to the First Protocol that are also Party 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 Party 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 to 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 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 Party 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 Party 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 the Protocol and co-operation under the 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. The 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 coordinating 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 10, 12, and 9. 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 also was 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, and in Explanatory Report paragraph 154, 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 the Protocol is consistent with that in other international instruments, such as the Convention for the Protection of Individuals with Regard to the Automated Processing of Personal Data (ETS No. 108), as amended by Protocol (ETS No. 223), the 2013 OECD Privacy Guidelines, the EU General Data Protection Regulation and 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 of 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 is not "personal data", such as anonymised information that cannot be reidentified without unreasonable time, effort or resources.

Article 4 – Language

47. This article 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. Further, 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 in 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 in its domestic law or treaties.

53. As used in paragraph 1, "requests, orders and accompanying information" refers to

a. 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);

b. 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)

c. 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 for purposes of Articles 7 and 6. This provision is designed to ensure swift co-operation and increased certainty without imposing 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, "Orders 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 submitted to service providers and entities providing domain name registration services under paragraph 2 of Article 4 and 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 provisions applicable to Chapter II

Article 5 – General principles applicable to Chapter II

62. Paragraph 1 of this article 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 2-5 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 also are 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 often are sought in the later stage 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 cooperation 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 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 for "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" (or "Emergency MLA"). Although Emergency MLA 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. 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 (governing mutual assistance in the absence of a treaty). See Article 10, paragraph 7.

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, like 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 the 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. This article 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 multi-stakeholder 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 to 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 for similar activities, fraud, distribution of child abuse materials, and 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 was 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 purposes of this article, 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 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 authorities" 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, this article 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. "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, email address and telephone number of a registrant. Some Parties may consider this information a subset of subscriber information as defined in Article 18.3 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 82 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 to requests under this article without difficulty, 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 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, email 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 submit 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 may only 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 this article.

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. This article 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 Convention Committee’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 18.3 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 geographical address, telephone or 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 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, that article 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). 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 this article 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 this article. 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 on Cybercrime). 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 this Article, 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 Explanatory Report paragraph 182 to the Convention).

98. As defined in paragraph 2.b of Article 3, the term "competent authorities" 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, this article 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 this article, 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 this article, 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 this article 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 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 in Article 14 safeguards required for that purpose.

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 96 above) in view 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 "the order under 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 this article 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, 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 the Protocol.

103. Regarding the difference between paragraph 3.a (the issuing authority) and 3.d (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 this article 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); 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 this Article.

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 of 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 this article 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, and Parties are obliged to ensure that the information is kept up to date, including where Parties change the single authority designated.

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 such 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 Secretariat of the Council of Europe is required to set up and keep current a register of all of the notification requirements under paragraph 5.e. Having a publicly available and an up-to-date register 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 Secretariat 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 email 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, in paragraph 4, and Article 8 in paragraph 5 also contain similar text.

Paragraph 7

117. Paragraph 7 provides that, if a service provider does not comply with an order issued under this article, 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 timeframe 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 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 92 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 data

124. The purpose of this article is for a requesting Party to have the ability to issue an order to be submitted as part of a request to a requested 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 this article, 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 this article 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 this article, as described in greater detail below.

128. In this article, 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 this article, 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, include the name of the service provider(s) to be served, a statement that it is being issued pursuant to this Protocol, 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)), the authority that issued the order, the authority seeking the data, and the offence that is the subject of the criminal investigation or proceeding. 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 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 provide efficiencies to the process. Included in the list of supporting information is:

a. under paragraph 3.b.i, the statutory basis for the issuing authority's authority 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;

b. under paragraph 3.b.ii, 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 the offence provision and its range of penalties is important for the requested Party to assess whether or not the request is within the scope of its obligations;

c. under paragraph 3.b.iii, any information that the requesting Party can provide that led it to conclude that the service provider(s) who is the subject of the order is in possession or control of the information or data sought. This information is key to initiating the domestic process. 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;

d. under paragraph 3.b.iv, a brief summary of the facts related to the investigation or proceeding. This information is also key for the requested Party to determine whether or not an order under this article should be given effect in its territory;

e. under paragraph 3.b.v, 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 requesting Party's specific criminal investigations or proceedings";

f. under paragraph 3.b.vi, 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;

g. under paragraph 3.b.vii, 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. The information under this subparagraph should include, for example, reference numbers and date of preservation. The 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 seek extension of preservations in a timely manner;

h. under paragraph 3.b.viii, information as to whether the data has already been sought by other means and 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 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 45 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 20 days and traffic data within 45 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, not meeting the return date for production, and 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 Explanatory Report paragraph 253 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. A 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 this article. 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 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 to obtain expeditiously in an emergency, 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 Explanatory Report paragraph 42 and 172, 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 email 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, for specific channels for rapidly expedited co-operation in emergency situations: this article 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 Network is staffed with points of contact who, in practice, communicate rapidly and without the need for written translations and are positioned 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 this article. 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, (1) little or no time may be lost by using that channel if there are particularly close working relations between the central authorities concerned; (2) emergency mutual assistance may be used to obtain additional forms of co-operation beyond computer data held by providers, and (3) 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 Explanatory Report paragraph 152 above, subject to the possibility of a declaration under Article 9, paragraph 5. The term “emergency” is defined in Article 3. Under the present Article, 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 incorporate 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 is stored or existing data and does not include data that has 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 this article 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 to other Parties of data in emergency situations.

160. It is within the discretion of the requested Party to determine: (1) whether the requirements for use of this article have been met; (2) whether another mechanism is suitable for purposes of assisting the requesting Party; (3) 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 7a, 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 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 accelerated 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 protocol Article 10, in that Article 25, paragraph 3, 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 protocol Article 10 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 above 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 it must include in its request a description of the facts that so demonstrate, and explain 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 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 request in electronic form. Before accepting the request, the requested Party may make the acceptance of the request conditional to 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 is evidence of the offence and the 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 24 hour a day, seven day a week basis, in case emergency requests must be made outside regular business hours. It should be recalled that in this regard the 24/7 network under Article 35 of the main Convention is available to coordinate 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 endeavor 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 alternate 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 transmission, maintain the integrity of the evidence, or other 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 determine, for example, to 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 of this article. Paragraph 7 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, this article is supplemented by the provisions of that agreement 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 Organisation

(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 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 investigations or proceedings – 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 of 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 Explanatory Report paragraph 145 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 (Second Additional Protocol to the Convention on Mutual Assistance in Criminal Matters). 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 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 coordination is essential. Additional coordination 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, etc. 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 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 coordination to initiate and maintain the transmission and have alternate 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 subparagraphs.

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, and Explanatory Report paragraph 38.

193. Paragraph 2.a 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 2-4 (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 appear, 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 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 case, 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 (1) fees of an expert witness; (2) costs of translation, interpretation and transcription, and (3) 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 on 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 such cost and how they can avoid such cost if the requesting Party cannot bear it.

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 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 hearings, ... such as identification of 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 6 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 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 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 coordination 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 coordination is otherwise useful.

203. As indicated in Article 5 of this Protocol and Explanatory Report paragraphs 182 to 186, the provisions of this article 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 this article – 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; the terms of gathering, transmitting and using information or evidence; terms of confidentiality; and terms of involvement of participating authorities of a Party in investigative activities shall be as agreed between the 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, 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 coordination – such as cases with particularly serious ramifications or situations raising particular problems of coordination – other appropriate channels may be agreed. For example, the central authorities for mutual assistance may be available to assist in coordinating 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 the 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-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.

214. It should be noted, that when paragraphs 6.a-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 person" is explained in more detail in the Explanatory Report paragraph 42 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 case 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 7, paragraphs 3 and 4; Article 6, paragraph 3; Article 8, paragraph 3; Article 9, paragraph 3). Additionally, the types of data to be disclosed are specified in each article, 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 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 the 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 that is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offenses and that 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 the Automated 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 the Convention for the Protection of Individuals with Regard to the Automated Processing of Personal Data (ETS No. 108), as amended by Protocol (CETS No. 223), this means that Article 14, paragraph 1, as further explained in paragraphs 105 to 107 of the Explanatory Report to that treaty, 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 II 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, the Protocol ensures appropriate protections for data transfers under the 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 the 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 the 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 consultations and suspensions, 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 this article is to establish appropriate safeguards permitting the transfer of personal data between Parties under the 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 the 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 the Protocol. Paragraph 2.a provides that "the Party that has received personal data ("receiving Party") shall process it for the purposes described in Article 2", that is, for the purpose of "specific 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 offenses 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, the 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 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, its 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 this article. 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 the Protocol, "the receiving Party shall ensure under its domestic legal framework that the personal data be relevant to and not excessive in relation to the purpose(s) for which it is processed." 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 is as up to date as is necessary and appropriate for, lawful processing of the personal data, having regard to the purposes for which it is processed." The context is important, so that this principle may be implemented differently in different situations. 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 the 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 the 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 is found to be incorrect or out-dated, 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 the 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 includes "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 results from chromosomal, DNA or RNA analysis and relates 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 includes “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 Convention, as further detailed in paragraphs 58 and 59 of that Convention’s 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 (a) 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 (b) 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, it 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 the 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 relates takes place in the investigation for which the data was 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 relates. 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 the 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 was 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 offenses 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 email 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 benefit 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 coordinated 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 its authority or authorities to be notified under paragraph 7.b for purposes of Chapter II, Section 2.

Paragraph 8 – Maintaining records

257. Paragraph 8 requires Parties to “maintain records on or have other appropriate means of demonstrating 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 has 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 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 this article. 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 the 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 the Protocol under Article 17, in accordance with the conditions set out therein. In line with paragraph 298 of the 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.” This is similar to 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 the 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 this article.

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 the 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 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 was 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 has been provided to another Party under the 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 has 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 has 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 has been received under the Protocol, and has been or is 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 is expected to be implemented by each Party in accordance with the relevant principles of its domestic legal framework. For Parties to the European Convention of Human Rights or to Protocol CETS No. 223 amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 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 case 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 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., an individual 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 has 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 to implement appropriate measures to minimise that risk. Parties are encouraged, when feasible, to notify the Party from which the data was received and other entities with whom the data has 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. 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 the Protocol to another Party when Parties are proceeding under paragraph 1.a of this article. 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 the 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, absent 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 a reasonable opportunity to clarify the situation or to address stated concerns. At the outset of such consultation, the Party invoking this paragraph 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 the 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 this article 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. The 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 the 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, the 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; the 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 the 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 this article 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 offenses. Therefore, paragraph 2 of this article was inserted to make plain that the 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 the Protocol.

293. This article 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. This article 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 that at least three out

of 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 who 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 explanatory report paragraph 316 of 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 were permitted to take a reservation to the obligations in Chapter II of the Convention (establishment of domestic criminal offenses 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 were 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 the Protocol. While the Convention provided no federalism reservation for mutual assistance, the majority of the Protocol's measures do not operate in the same manner as traditional mutual assistance. The 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, the Protocol introduces two measures, Article 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, the 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 the Protocol, it may be the case that (1) they are operating under different procedural and privacy laws than those under which the central government authorities operate; (2) they do not answer to the central government in terms of organisational hierarchy; or (3) 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 the Protocol – those related to seeking information or evidence as well as those relating to the subsequent handling of such information or evidence – if (a) it applies them itself, or (b) 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 the Protocol (subject to available reservations and declarations). With respect to data protection obligations under the 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 237) where a federal authority has sought information under the 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 the Convention Article 41, paragraph 1, 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 "notified the Secretary General of the Council of Europe that the 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 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; 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 the 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 the 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 seeks and receives 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 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 1) inform the authorities of its constituent States or other similar territorial entities of the provisions of this Protocol; and 2) 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 the Protocol. For the 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. This article automatically applies the Protocol to territories specified by a Party under Article 38, paragraph 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 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, specify that this Protocol shall not apply to one or more territories specified in the Party's declarations under Article 38, paragraphs 1 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 the Protocol to additional territories that were covered under the Convention but to which the Protocol had previously not been applied.

308. This article does not permit applying the 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 Explanatory Report paragraph 315 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 this article 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 this article to traffic data.

312. This article also refers to declarations. Similarly 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).

314. A second category of declarations permits Parties to require separate or additional procedural steps for certain measures or 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 are to be addressed only to its central authority – other Parties must address requests to the declaring Party's Central Authority, but the declaring Party need not 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, paragraph 5.a and e., and Article 8, paragraphs 4 and 10.a and b, 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 under paragraph 5.a is first given, communicate to the Secretary General of the Council of Europe 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, paragraph 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 it provides 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. This article 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, "the 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 this article 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 agreed by the Parties, 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 as appropriate, to take into account needs that may arise from the implementation of this Protocol.

321. Similar to the Convention (see Explanatory Report paragraph 327), 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 the 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 and 1.c. 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 this article 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 "the 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 the 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 the Protocol, at which point the Parties may modify these procedures. 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 this article 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 this article 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 paragraph 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 that 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."