COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, version 10 November 2020 T-CY (2018)23rev

Cybercrime Convention Committee (T-CY)

Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime

Provisional text of provisions:

- **Language**
- **Video conferencing**
- **Joint investigation teams and joint investigations**
- **Direct disclosure of subscriber information**
- **Giving effect to orders from another Party for expedited production of data**
- **Request for domain name registration information (NEW)**
- **Expedited disclosure of stored computer data in an emergency (NEW)**
- **Emergency MLA**

www.coe.int/cybercrime

Contents

1 Language[1]

1.1 Draft text[2]

Article [ ] – Languages of requests

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

2. For purposes of Articles [direct disclosure], [preservation], and [emergency disclosure], an order [or request][3] and accompanying information[4] submitted directly to a service provider in the territory of another Party shall be:

   a. submitted in a language of the other Party in which the service provider accepts comparable domestic process;
   b. submitted in another language acceptable to the service provider; or
   c. accompanied by a translation into one of the languages under subparagraphs (a) or (b).

1.2 Draft Explanatory Report

1. This Article provides a framework for languages that may be used when addressing Parties and service providers. 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.

2. Inaccurate or costly translations of mutual assistance requests relating to electronic crime 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 [ ], or requests to give effect to an order under Article [ ]. While machine translation capabilities are expected to improve, they are currently inadequate. For these reasons, the translation problem was mentioned repeatedly in proposals about the articles to include in a protocol.

3. 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 countries. However, the cost and difficulty of translations fall disproportionately on requesting Parties where less-common languages are spoken.

4. Because of this disproportionate burden, a number of non-Anglophone countries asked that English be mandated in a protocol. They noted that English is a commonly used language by major service providers. Further, as data is 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. Drafters particularly emphasized that, to speed assistance, all efforts should be made to

[1] **Revised text** as agreed provisionally by the PDP, Strasbourg, 8 November 2019. Text may change as the Protocol evolves and comments are received.
[2] **NOTE**: A general provision on scope needs to be included: The provision covers any form of request under Articles 24 through 34, inclusive, of the mother convention and under the two protocols ….
[3] Review later on: eg process re preservation etc.
[4] review in provision on direct disclosure to "supporting information" versus "additional information".

accept preservation requests and, in particular, emergency requests under this Protocol, in English or a shared language rather than in translation.

5. The drafters of the Protocol concluded that English should not be mandated in the treaty text. Some countries have official-language requirements that preclude such a mandate; many countries share a language and have no need for English; and, in some countries, officials outside of capitals are less likely to be able to read English but are often involved in executing requests.

6. Thus, paragraph 1 is phrased in terms of "a language acceptable to the requested Party or the Party notified under Article [direct disclosure]." 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.

7. As used in paragraph 1, "requests, [and] orders and accompanying information" refers to

a. under Article [endorsement], 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 [direct], the order, supporting information, and the summary (paragraph 5.a).

"Requests" also refers to the contents of mutual assistance requests under Articles [emergency MLA], [video conferencing], [ ] which includes documentation that is part of the request.

8. 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 the second protocol.

9. This pragmatic provision demonstrates the extreme importance of speeding up cooperation. It provides a treaty basis for a Party to accept additional languages for purposes of this protocol.

10. 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 [direct]," 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.

11. A Party's willingness to accept other languages will be reflected via its indication to the T-CY that it agrees to accept some or all types of requests or notification of orders under this Protocol in another language.

12. Paragraph 2 is limited to determining the language(s) the issuing party will use to submit orders [or requests] and accompanying information to service providers. It specifies the language(s) in which a Party shall submit an order [or request] directly to a service provider in another Party's territory for purposes of Articles [direct], [preservation], and [emergency disclosure]. It provides options to determine the language(s) in which the requesting State can submit an order [or request] to a service provider in another Party's territory. This provision is designed to ensure swift cooperation and increased certainty without imposing additional burden on service providers when they receive orders [or requests] to disclose [or preserve] data. The first option indicates that the order [or

request] can be submitted in a language in which the service provider usually accepts domestic orders [or requests] from its own authorities in the framework of 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 indicates that if a service provider agrees to receive orders in another language, e.g. the language of its headquarters, such orders and accompanying information can be submitted in that language. As a third option, where the order and accompanying information is not issued in one of those languages, it shall be accompanied by a translation into one of those languages.

13. As used in paragraph 2, "orders [and requests] and accompanying information" refers to the order (paragraph 3) and the additional information (paragraph 4) under Article [direct].[5]

14. Where a Party has required notification pursuant to Article [direct], 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.

15. The T-CY will also informally endeavour to gather information on the languages in which [requests and] orders and accompanying information shall be made to service providers under paragraph 2 of the Article and make Parties aware of them as part of the survey described in paragraph [7] of the Explanatory Report, above.

[5] This may need to be further adjusted should articles on preservation and emergency disclosure be included in the Protocol.

2 Video conferencing[6]

2.1 Draft text

Article [ ] – 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 instructions to the witness or expert; the manner of questioning of the witness or expert; the manner to ensure due respect for the rights of the witness or expert; the treatment of claims of privilege or immunity; the treatment of objections to questions or responses; and whether one or both Parties shall provide interpretation and transcription services.

2. A requested Party providing assistance under this article shall endeavor 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.

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

4. Without prejudice to any jurisdiction under the 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 law of the requested Party, obliged such person to testify truthfully; or
   b. refuses to testify when the requested Party has, in accordance with the law of the requested Party, obliged such person to testify; or
   c. commits other misconduct that is prohibited by the 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 conduct had been committed in the course of its domestic proceedings.

5. a. Unless otherwise agreed 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.

[6] Text as agreed provisionally by the PDP, Strasbourg, 29 November 2018. Text may change as the Protocol evolves and comments are received.

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

6. 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 hearings, other than those described in paragraph 1, including for purposes of identification of persons or objects.

7. 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.

2.2 Draft Explanatory report

1. Article [ ] primarily addresses the use of video conferencing technology to take testimony or statements. This form of cooperation may be provided for in existing bilateral and multilateral mutual assistance treaties, e.g., ETS 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, Article [ ], like several other articles in this Protocol, applies in the absence of a mutual legal assistance treaty, or arrangement on the basis of uniform or reciprocal legislation, in force between the requesting and requested Parties. Such articles follow the same approach as in Article 27 of the Budapest Convention.

2. In addition, Article [ ] has the same material scope as in Article 25 of the Budapest Convention, that is, it is available "for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence." As stated in paragraph 253 of the Explanatory Report to the Budapest Convention, "criminal offences related to computer systems and data" means "the offences covered by Article 14, paragraph 2, litterae a-b" of the Budapest Convention, i.e., "the criminal offences established in accordance with Articles 2-11 of this Convention" and "other criminal offences committed by means of a computer system ...."

3. Paragraph 1 authorizes 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, 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.

4. At the same time, it is expected that parties to the Protocol will have the basic technical capability to provide assistance via video conferencing.

5. 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 (e.g., 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 should be discussed and agreed 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, it is advisable to discuss in advance 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.

6. 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 2, where the requested Party provides assistance under this article, it must endeavor 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 legal framework 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 authorizes it to do so, in accordance with the safeguards set forth in its domestic law.

7. The procedure relating to the conduct of video conferences is set forth in paragraph 3. 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.

8. The purpose of paragraph 4, 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 (e.g., 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 (e.g., 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.

9. Paragraph 5 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 subparagraph (b) of this Paragraph, 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.

10. While paragraph 1 expressly authorizes the use of video conferencing technology for taking testimony or statement, subparagraph (a) of paragraph 6 provides that the provisions of Article [ ] may be applied for purposes of carrying out audio conferences where so mutually agreed. In addition, subparagraph (b) of paragraph 6 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.

11. Paragraph 7 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 7 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.

3 Joint investigation teams and joint investigations[7]

3.1 Draft text

Article [ ] – 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 investigations or prosecutions, 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; organization; gathering, transmission and use of information or evidence; and terms of involvement of participating authorities of a Party in investigative activities taking place in another Party's territory, shall be as agreed between those competent authorities.

3. Those competent and participating authorities shall communicate directly, except that Parties may agree on other appropriate channels of communication where exceptional circumstances require more central coordination.

4. 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.

5. 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 offenses 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. for them to prevent a situation in which there is a significant and imminent threat involving the life or safety of a natural person.8 In that case, the participating authorities that received the information or evidence shall notify

[7] Text as agreed provisionally by the PDP via written procedure, Strasbourg, 15 May 2020. Text may change as the Protocol evolves and comments are received.
[8] The definition/concept of "emergency" will need to be aligned when other provisions referring to emergencies (Emergency MLA, [Disclosure of content in emergencies]) will be finalised.

the participating authorities that provided the information or evidence without undue delay, unless mutually determined otherwise.

6. 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 [and in accordance with applicable domestic conditions and safeguards].[9]

3.2 Draft Explanatory Report

1. 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 cooperation or coordination between two or more States. Article [ ] provides a basis for such forms of cooperation.

2. 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.

3. As indicated in Article [general principles re this chapter] of this Protocol and explanatory report paragraphs [x to y], [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 agree to apply any or all of the remainder of this Article in lieu thereof].[10]

Paragraph 1

4. 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.

5. 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 prosecutions to enter into such an agreement; others may require the central authority – the office normally responsible for mutual legal 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.

6. [It is expected that Parties to the Protocol will have the ability to engage in this form of cooperation as stipulated in Article 25.2 of the Convention.[11]]

Paragraph 2

7. 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; gathering, transmission and use of information or evidence; 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 and what procedure to follow if the information or evidence is needed for purposes other

[9] Text in [brackets] to be reconsidered in the light of the overall approach to safeguards in the Protocol.
[10] Note: To be reviewed once Article [on general principles of this Chapter] has been drafted.
[11] Note: This paragraph may be placed in more general section on MLA.

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 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.

8. It is anticipated that Parties will generally agree in writing regarding these procedures and conditions. 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.

9. 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 cooperative measures under the Protocol, Article [safeguards] [may / should[12]] apply to the transfer of personal data pursuant to JITs.

10. As generally is the case with respect to all information or evidence received by a Party pursuant to the Protocol, that Party's applicable rules of evidence will govern whether the information or evidence will be admissible in judicial proceedings.

Paragraph 3

11. Under paragraph 3, the competent authorities determined by the Parties under paragraph 1 and the participating authorities described in paragraph 3 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 legal assistance may be available to assist in coordinating such matters.

Paragraph 4

12. Paragraph 4 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 5

13. Paragraph 5 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 subparagraphs a-c. The circumstances set out in paragraph 5 are without prejudice to the requirements set out for onward transfers of information or evidence to another State in Article [data protection safeguards].

[12] Note: "may" or "should" to be determined once the article on data protection safeguards is finalised.

14. It should be noted, that when subparagraphs 5.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.

15. In subparagraph 5.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.

16. The drafters understood that subparagraph 5.c refers to exceptional circumstances where the receiving Party's authorities could directly use the information or evidence to prevent a significant and imminent risk to the life or safety of any natural person. 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 in [Para. 2] of Article [Emergency mutual assistance] 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.[13] In case information or evidence is used under subparagraph 5.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 6

17. Lastly, it should be generally recalled that there is a long history of international cooperative 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 cooperated with foreign counterparts in a particular investigation, other than on the basis of a JIT. Paragraph 6 provides for these international cooperative efforts and provides a treaty basis for entering into a joint investigation in the absence of an agreement described in paragraphs 1-2 should a Party require such a legal basis. [Parties entering into a joint investigation under paragraph 6 should apply applicable conditions and safeguards under their domestic laws.] [14]

[13] The definition/concept of "emergency" will need to be aligned when other provisions referring to emergencies (Emergency MLA, [Disclosure of content in emergencies]) will be finalised.
[14] Text in [brackets] to be reconsidered in the light of the overall approach to safeguards in the Protocol.

4 Direct disclosure of subscriber information

Note: The PDP has provisionally adopted the following text and explanatory report by 30 September 2019, subject to the understanding that they may change as the negotiations develop, depending on the outcome of other provisions that have not yet been prepared and/or other comments received. In particular, in view of the unique circumstances of direct cooperation between authorities and providers, once the ongoing work on conditions and safeguards, including with regard to data protection and privacy, has resulted in a text and explanatory report, this article and its explanatory report should be considered by the PDG and PDP in order to determine whether further changes are required.

4.1 Draft text

Article [ ]: 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, to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the 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 or when depositing its instrument of ratification, acceptance, approval or accession, a Party may – with respect to orders issued to service providers in its territory - make the following declaration: "the order under Article [ ] 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 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 additional information:

   a. the domestic legal grounds that empower the authority to issue the order;
   b. reference to legal provisions and applicable penalties for the offence being investigated or prosecuted;
   c. contact information of the authority to which the service provider shall return the subscriber information, request further information, or otherwise respond;
   d. the time and the manner in which to return the subscriber information;
   e. whether preservation of the data has already been sought, including date of preservation and any applicable reference number;
   f. any special procedural instructions; and

g. any other information that may aid in obtaining disclosure of the subscriber information.

5. a. A Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, 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 simultaneous notification, in every case or in identified circumstances, of the order, the supporting 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 with under paragraph 5.b may, without undue delay, instruct the service provider not to disclose the information if:

i. disclosure may prejudice criminal investigations or proceedings in the receiving Party; or
ii. conditions or grounds for refusal would apply under Articles 25.4 and 27.4 of the Convention if the subscriber information had been sought through mutual assistance.

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

i. may request additional information from the issuing Party for the purposes of applying paragraph 5.c;
ii. shall promptly inform the issuing Party if the service provider has been instructed not to disclose the information and give the reasons for doing so.

e. For the purposes of paragraph 5, a Party shall designate a single authority to receive notification under paragraph 5.a and perform the duties related to consultations described in paragraphs 5.c. and 5.d. The Party shall, at the time of signature, or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the 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 held on the register are correct at all times.

6. A Party may submit an order under paragraph 1, additional information under paragraph 4 and notification under paragraph 5 in electronic form. However, 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 30 days of receipt of the order or the timeframe stipulated in subparagraph 4.d, whichever time period is longer, the competent authorities of the issuing Party may then seek to enforce the order only

via Article [Giving effect to orders from another Party for expedited production of data] or other forms of mutual assistance. Parties may request that a service provider give a reason why the provider is not disclosing subscriber information sought by the order.

8. A Party may declare that another Party shall seek disclosure of subscriber information from the service provider before seeking it under Article [Giving effect to orders from another Party for expedited production of data], unless the issuing Party provides reasonable explanation for not having done so.

9. 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.

4.2 Draft Explanatory Report

Article [ ]: Disclosure of subscriber information

1. This article establishes a procedure that provides for the direct cooperation 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 criminal investigations and proceedings, in view of the challenges posed by existing procedures for obtaining electronic evidence from service providers in other countries.

2. An increasing number of criminal investigations and proceedings nowadays require access to electronic evidence from service providers in other countries. Even for crimes that are entirely domestic in nature – i.e., 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 cooperation 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.

3. 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.

4. Subscriber information is defined in Article 18.3 of the Convention as including "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 . . ." (see also Explanatory Report of the Convention on Cybercrime, paragraphs 178-180). 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.

5. While Article 18 of the Budapest 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 18.1.a of the Convention) or "offering its services" in the issuing Party (see Article 18.1.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 criminal investigations and 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 cooperation between authorities of one Party with service providers located in another Party.

6. As reflected in Article [general rules on relationship with the Convention], this Article is without prejudice to the ability of Parties to enforce orders issued under Article 18 or otherwise as permitted by the Convention, or prejudice cooperation (including spontaneous cooperation) between Parties, or between Parties and service providers, through other applicable agreements, arrangements, practices or domestic laws.

Paragraph 1

7. 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.

8. Paragraph 1 also includes the requirement that the orders may only be issued and submitted in the context of an issuing country's own "specific criminal investigations or proceedings," as that phrase is used in Article 14(1) of the Convention (see paragraphs 140 and 152 of the Explanatory Report to the Convention on Cybercrime). 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 – i.e. 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 (i.e., 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 reemphasizes the principle already set by Article 18 of the Convention, that the provisions may not be used for mass or bulk production of data.

9. Paragraph 138 of the Explanatory Report to the Budapest Convention provides that 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 procedural measure. The same approach is foreseen for purposes of the direct cooperation procedure in this Article. Accordingly, the national 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 cooperation, as described further below.

10. 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

11. In paragraph 2 of the 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 national legal systems, Parties may implement different measures to establish a procedure for the direct cooperation 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 authorize eventual international transfers of the responsive subscriber information, this Protocol reflects the important public interest of this direct cooperation measure and includes in Article [ ] safeguards required for that purpose.

12. As explained in paragraph 9, Paragraph 138 of the Explanatory Report to the Budapest Convention provides that 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 procedural measure. The same approach is foreseen for purposes of the direct cooperation procedure in this Article. Accordingly, the national 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 [8] above) in view of the direct nature of the cooperation. 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 the enumerated authorities.

Paragraph 3

13. Paragraph 3 of the article specifies the information that, at a minimum, shall be provided by an authority issuing an order pursuant to paragraph 1 of the 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.

14. Regarding the difference between subparagraph a. (the issuing authority) and d. (the authority seeking the subscriber information), in some countries, 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.

15. 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

16. 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 additional information. Therefore, paragraph 4 of the article specifies that an issuing authority shall provide additional 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 (e.g. 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 additional information can be provided separately but also may be included in the order itself, if this is permissible under the issuing Party's law. Both the order and the additional information shall be transmitted directly to the service provider.

17. 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. 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.

Paragraph 5

18. Under paragraph 5.a, a Party may notify the Secretary General of the Council of Europe that, when it is the receiving Party, it will require the issuing Party to simultaneously notify it of any order sent directly to a service provider in its territory either in every instance (i.e., for all orders transmitted to service providers in its territory), or in identified circumstances.

19. 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 significantly delay compliance with requests, 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 receiving Party's criminal investigations or proceedings.

20. The notification and consultation procedures are entirely discretionary. A Party is not obligated to require either procedure.

21. Receiving Parties 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 [18 of the Explanatory Report on Article [giving effect]]. Because of this, the ability of a Party to be notified or consulted provides an additional safeguard. That said, cooperation 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 and provide for more efficient and expedited procedures for cross-border access to electronic evidence for criminal investigations.

22. Implementation of this Article – including the extent to which a Party should be able to rely on the grounds for refusal – is affected by other provisions, for example, the scope of application, and conditions and safeguards (including with respect to data protection). The operative text and explanatory report pertaining to such other articles provide detail regarding the manner in which this article is affected.

23. 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 issuing authority 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 receiving Party's authorities must gather the necessary information and make their determination "without undue delay." They must also notify the issuing Party's authorities promptly in the event that they decide to instruct the service provider not to comply, as well as provide the reasons for doing so.

24. 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.

25. Pursuant to paragraph 5.e, a Party requiring notification or consultation must identify a single authority and provide the Secretary General of the Council of Europe with adequate contact information.

26. A Party may change its notification 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 cooperation 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 cooperation mechanism, it wishes to institute a notification or consultation regime.

27. 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 and of the authorities with which providers consult under paragraph b. 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 and consultation 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 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

28. Paragraph 6 makes clear that serving an order or notifying another Party using electronic means, including use of e-mail and electronic portals, is permissible. The goal is to encourage the use of electronic means where not prohibited by law, 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 (e.g. 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 3 of Article [Emergency mutual assistance], and further guidance with respect to the security requirement is provided in paragraph [ ] of the Explanatory Report. Article [Giving effect to orders from another Party for expedited production of data] also contains a similar text in paragraph 5.

Paragraph 7

29. 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 [Giving effect to orders from another Party for expedited production of data] or another form of mutual assistance. Parties proceeding under this Article may not seek unilateral enforcement.

30. For enforcement of the order via Article [Giving effect to orders from another Party for expedited production of data], the Protocol contemplates a simplified procedure of conversion of an order under this Article to an order under Article [Giving effect to orders from another Party for expedited production of data] to facilitate the ability of the issuing Party to obtain subscriber information.

31. In order to avoid duplication of efforts, an issuing Party must give the service provider 30 days or the timeframe stipulated in subparagraph 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 [Giving effect to orders from another Party for expedited production of data]. 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 is no longer available.

32. 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 [Giving effect to orders from another Party for expedited production of data] 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 [Giving effect] or via any other mutual assistance mechanism that may be rejected.

Paragraph 8

33. 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 [Giving effect to

orders from another Party for expedited production of data] 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 [Giving effect to orders from another Party for expedited production of data], and, as a result, could reduce the number of situations in which Article [Giving effect to orders from another Party for expedited production of data] needs to be invoked. Article [Giving effect to orders from another Party for expedited production of data] 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 [Giving effect to orders from another Party for expedited production of data] to both categories of data, the issuing Party would not need to first seek the subscriber information separately.

Paragraph 9

34. 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.

35. Paragraph 9.b provides that – for the reasons explained in paragraph [4] 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.

5 Giving effect to orders from another Party for expedited production of data

Note: The PDP provisionally adopted the following text and explanatory report on 11 July 2019, subject to the understanding that they may change as the negotiations develop, depending on the outcome of other provisions that have not yet been prepared and/or other comments received. In particular, once the ongoing work on conditions and safeguards including with regard to data protection and privacy, has resulted in a text and explanatory report, this article and its explanatory report should be considered by the PDG and PDP in order to determine whether further changes are required.

5.1 Draft Text

Article [ ]: Giving effect to orders from another Party for expedited production of 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 to another Party (requested Party) for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored

    a. subscriber information,
    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 another Party (requesting Party).

3. 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 date 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 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. 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 to provide further information;
vii. whether preservation of the information or data has already been sought, including date of preservation and any applicable reference number; and
viii. whether the data has already been sought by other means, and 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 or when depositing its instrument of ratification, acceptance, approval or accession, 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. However, 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 45 days, if not sooner, and shall order a return of production no later than:

i. 20 days for subscriber information; and
ii. 45 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 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 or impose terms and conditions on the execution of a request on the grounds established in Article 25.4 or Article 27.4 of the Convention. The requested Party may postpone execution of requests for reasons established under Article 27.5. In either case, the requested Party shall notify the requesting Party as soon as practicable of the refusal, terms or 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.

9. Every Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe 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.

10. A Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it requires that requests under this

Article be transmitted by the central authority or authorities of the requesting Party, or by such other authority as agreed between the Parties concerned.

11. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 9. Each Party shall ensure that the details held on the register are correct at all times.

12. A Party may reserve the right not to apply this Article to traffic data.

5.2 Draft Explanatory Report

Article [ ] Giving effect to orders from another Party for expedited production of data

1. The purpose of this Article is for a requesting Party to have the ability to issue an order to be submitted 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.

2. The 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.

3. 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 authorized in law and that can be issued for the purpose of compelling the production of subscriber information or traffic data.

4. Although "competent authority" for the purposes of the Convention is discussed in the Explanatory Report to the Convention (at para 138), it is not defined in the Convention. Similar to what is explained in paragraph 138 of the Explanatory Report of the Convention, "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, authorize or undertake the execution of procedural measures 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 9 of this Article, as described in greater detail below.

5. 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.

6. Paragraph 2 requires the requested Party 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.

7. While the 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.

8. 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 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 under Article 27.8 of the Convention, at the time of transmission to ensure the proper processing of the request.

9. 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 (i.e., 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 (Article 18.3 of the Budapest Convention); 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 (Art. 1.d of the Budapest 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.

10. 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 the Article have been met, i.e, that the information or data is "needed for the requesting Party's specific investigations or proceedings";
f. under paragraph 3.b.vi, the contact information of an authority or authorities in case the designated 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 is 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 ensure that preservation is extended 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.

11. 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.

12. 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.

13. 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.

14. 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 laws, 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.

15. The purpose of paragraph 5 is to encourage Parties to use secure and authenticatable means of electronic communications to facilitate the transmission of information or data and documents, including transmission of orders and supporting information, and the sending of the produced information or data and documents (see paragraph [4 of the Explanatory Report to the provision on emergency mutual assistance]).

16. Under paragraph 6, the requested Party should take reasonable steps efforts 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 Parties 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.

17. 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.

18. Under paragraph 8 the requested Party may refuse to proceed with any part of the process that gives effect to the requesting Party's order, or determine that only part of the order can be given effect depending on the circumstances of the case, or deny the request entirely, if the grounds for refusal established in Articles 25.4 or 27.4 of the Convention exist. In addition, the requested Party may postpone execution of the order under Article 27.5 of the Convention. The requested Party shall notify the requesting Party of its decision to refuse or postpone any part of the request.

19. Implementation of this Article – including the extent to which a Party should be able to rely on the grounds for refusal – is affected by other provisions, for example, the scope of application, and conditions and safeguards (including with respect to data protection). The operative text and explanatory report pertaining to such other Articles provide detail regarding the manner in which this Article is affected.

20. It should be recalled that the Explanatory Report paragraph 253 of the Budapest 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.

21. The purpose of paragraph 9 is to ensure that Parties, at the time of signature, or when depositing their instruments of ratification, acceptance, approval, or accession, 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.

22. Paragraph 10 permits a Party to declare that it requires that orders submitted to it under this Article be transmitted by a central authority of the requesting Party, or other authority where agreed between the Parties. Any central authority or authorities designated by the requesting Party in accordance with Article 27.2.a of the Convention may transmit such an order. Parties are encouraged to provide as much flexibility as possible for the submission of requests.

23. Paragraph 11 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 9 and for each Party to ensure that the details held on the register are accurate. Such information will assist requested Parties to verify the authenticity of requests.

24. Under paragraph 12, 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.

6 Request for domain name registration information

Note: The PDP provisionally adopted the following text and explanatory report on 9 November 2020, subject to the understanding that they may change as the negotiations develop, depending on the outcome of other provisions that have not yet been prepared and/or other comments received. In particular, once the ongoing work on conditions and safeguards including with regard to data protection and privacy, has resulted in a text and explanatory report, this article and its explanatory report should be considered by the PDG and PDP in order to determine whether further changes are required.

6.1 Draft text

Article [ ]: 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 purposes of specific criminal investigations or proceedings[15],] to issue a request to an entity providing domain name 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 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 and that the need for the information arises because of its relevance to a specific criminal investigation or proceeding;
    d. the time and the manner in which to disclose the information and any other special procedural instructions.

4. [The information disclosed in response to a request under paragraph 1 shall be subject to appropriate safeguards pursuant to Articles 15 and [data protection].][16]

5. In the event of non-cooperation 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.

[15] This may be part of an overarching provision; to be coherent with other articles.
[16] Review the need to include this paragraph in the context of the overall review of safeguards in the protocol.

6.2 Draft Explanatory Report

1. This article establishes a procedure that provides for the direct cooperation between the authorities of one Party and an entity providing domain name services in the territory of another Party to obtain information about internet domain name registrations. Similarly to Article [disclosure of subscriber information], the procedure builds on the conclusions of the Convention Committee's Cloud Evidence Group, acknowledging the importance of timely cross-border access to electronic evidence in criminal investigations and proceedings, in view of the challenges posed by existing procedures for obtaining electronic evidence.

2. 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 the Second Additional Protocol, that is, specific criminal investigations and proceedings. Obtaining the domain name registration data is often indispensable as a first step for many criminal investigations, and in order to determine where to direct requests to for international cooperation.

3. Many forms of cybercrime are facilitated by offenders creating and exploiting domains for malicious and illicit purposes. For example, a domain name may be used as a platform for the spreading of malware, botnets, phishing and similar activities, fraud, distribution of child abuse materials, and 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.

4. Domain name registration information is held by entities providing domain name 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 services (the registrar or registry) is located or where the person to whom the data relates is located.

5. The objective of the Article [Request for domain name registration information] 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

6. Under paragraph 1, each Party shall adopt measures necessary to empower its competent authorities to issue requests directly to an entity providing domain name 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 legal system, 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 cooperation under this Article and, if the entity does not disclose the information sought, paragraph 5 would be applicable.

7. 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, the Article uses technology-neutral terms to permit adaptation to evolving technology.

8. As foreseen in Article [general scope provision] of this Protocol, a request under paragraph 1 may be issued only for the purposes of specific criminal investigations and proceedings. In addition, the term "competent authorities" is given the same meaning as in Paragraph 138 of the Explanatory Report to the Convention in that it "refers to a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of procedural measures". An "entity providing domain name 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 services".

9. While information for identifying or contacting the registrant of a domain name is often stored by entities providing general domain name services globally, e.g. "generic top level domains" (gTLDs), Parties acknowledged that more specific domain name 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 services – or future types of such services – can be used to perpetrate cybercrime.

10. "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

11. Paragraph 2 requires each Party to adopt measures to permit entities in its territory providing domain name services to disclose such information in response to a request under Paragraph 1 subject to reasonable conditions provided by domestic law. These measures should facilitate the disclosure of the requested data in a rapid and effective manner to the greatest extent possible.

12. At the same time, 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 services may need to determine whether to disclose the information sought. The 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:

- the Protocol provides or requires Parties to provide a legal basis for requests;
- this Article requires that the request emanate from a competent authority [operative paragraphs 1 and 3.a and ER paragraph [ ]];
- the Protocol provides that a request is made for the purposes of specific criminal investigations or proceedings [article general provisions];
- 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 [operative para 3.c];
- the Protocol provides for safeguards for the processing of personal data disclosed and transferred pursuant to such requests through Article [Conditions/Safeguards];

- 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 cooperate under contractual arrangements with ICANN.

Paragraph 3

13. Paragraph 3 of the article specifies the information that, at a minimum, shall be provided by an authority issuing a request pursuant to paragraph 1 of the article. This information is particularly relevant for the execution of the request by the entity providing domain name services. The request will need to include:

a. The date of the request and the identity and contact details of the authority issuing the request (subparagraph a.), which must be a competent authority as described in paragraph [8] of the Explanatory Report to issue such requests according to paragraph 1 of the Article;
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 (subparagraph 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 the Protocol (subparagraph c.). The requesting Party also confirms in this statement that the information is "needed" because of its relevance to a specific criminal investigation or proceeding. For European countries, what information is "needed" – i.e. 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 (i.e., 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 (subparagraph d.). "Special procedural instructions" is intended to refer to 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 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.

14. 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

15. In view of requirements under data protection laws of certain Parties to authorise international transfers of the responsive information under this Article, this Protocol includes in Article [data protection] required for that purpose.]

Paragraph 5

16. 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. 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.

7 Expedited disclosure of stored computer data in an emergency

Note: The PDP has provisionally adopted the following text and explanatory report by 20 October 2020, subject to the understanding that provisions may change as the negotiations develop, depending on the outcome of other provisions that have not yet been prepared and/or other comments received. In particular, once the ongoing work on conditions and safeguards, including with regard to data protection and privacy, has resulted in a text and explanatory report, this article and its explanatory report should be considered by the PDG and PDP in order to determine whether further changes are required.

7.1 Draft text

Article [ ]: Expedited disclosure of stored computer data in an emergency

1. a. Each Party shall adopt such legislative and other measures as may be necessary for its Point of Contact for the 24/7 Network referenced in Article 35 of the Convention ("Point of Contact") in an emergency as defined in Article [emergency MLA], 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 declare that it will not execute requests under subparagraph a. seeking the disclosure only 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 subparagraph 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 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 the subject of the criminal investigation or proceeding and a reference to its legal provisions and applicable penalties;
   e. sufficient facts that 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 aid in obtaining disclosure of the requested data.

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

5. A Party may 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. When a Requested Party determines that it will not provide requested data to a Party that has made a request under 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 any other forms of cooperation that may be available.

7.2 Explanatory report

Introduction

1. In addition to the other forms of expedited cooperation provided for in the 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 paragraphs [Emergency MLA], the need for maximum expedited cooperation may arise in a variety of time-sensitive 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.

2. Under the Convention, in an emergency, Parties make mutual assistance requests to obtain data, and, under Article 35(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 legal assistance request.

3. As reflected in Article [general rules on relationship with the Convention], this Article does not prejudice cooperation (including spontaneous cooperation) between Parties, or between Parties and service providers, through other applicable agreements, arrangements, practices or domestic laws. Therefore, under the Protocol, all of the above mechanisms remain available to competent authorities that seek data in an emergency. The innovation of the Protocol is the elaboration of two Articles that obligate all Parties to provide, at a minimum, for specific channels for rapidly expedited cooperation in emergency situations: this Article and Article [Emergency mutual assistance].

4. This Article permits Parties to cooperate 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 legal framework. 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 legal framework 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.

5. Using the channel established in this Article may have advantages over the emergency mutual assistance channel set forth in Article [emergency mutual assistance]. 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 cooperation 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

6. 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 [general provisions] the request must be made pursuant to a criminal investigation or proceeding.

7. 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 as described in ER paragraph 5 above, subject to the possibility of a declaration under operative paragraph 5. The term "emergency" is defined in Article [emergency MLA].[17] Under the present Article, the requested Party will determine whether an "emergency" exists in relation to a request using the information provided in paragraph 3.

8. As opposed to other articles in this Protocol, such as Article [Direct disclosure], 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. 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 Convention ER para. 170.)

9. 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.

[17] Note: The definition/concept of "emergency" and the term "serious harm" as referred to in this and other provisions [Emergency MLA, JITs] will need to be aligned. In that connection, the explanatory report to Article [Emergency MLA] should be reviewed to ensure that the description of serious harm is consistent with national practices in this area.

10. 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 Art. 18.3 of the Convention. 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 [direct cooperation] or [giving effect], 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

11. Paragraph 2 requires that each Party adopt measures as necessary to ensure that its domestic legal framework permits its authorities 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.

12. 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.

13. 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 under its domestic legal framework 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 the 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

14. 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.

15. With regard to subparagraph 3.a., the requesting Party shall specify the competent authority on whose behalf the data is sought.

16. With regard to subparagraph 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 the Protocol and that any data obtained as a result will be handled in a manner consistent with the requirements of the Protocol. This will also differentiate the request from other emergency disclosure requests the 24/7 Network Point of Contact might receive.

17. Under subparagraph 3.e, the requesting Party must provide sufficient facts that demonstrate the existence of an emergency, as defined in Article [Emergency MLA], 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 under its domestic legal framework, it should consult with the requesting Party's 24/7 Network Point of Contact.

18. 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 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 shall, in consultation with the authorities of the requesting Party, determine when and in what manner confirmation of authenticity should be provided.

19. 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

20. The purpose of paragraph 4 is to encourage Parties to use rapid means of communication to facilitate the transmission of information or data and documents, including transmission of requests and the sending of the produced data. This paragraph is based on paragraph [] of [giving effect] 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

21. 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 disclosure of data. For some Parties such a procedure would be required by their domestic laws, whereas other Parties indicated that they have no such requirements and do not need to avail themselves of this possibility for a declaration.[18]

Paragraph 6

22. 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 [emergency mutual assistance] or another means of cooperation 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 cooperation that may be available, in an effort to achieve the Parties' mutual goal of expediting disclosure of data in emergencies.

[18] Check declarations throughout the Protocol.

8 Emergency mutual assistance[19]

8.1 Draft text

Article [ ] – Emergency Mutual Assistance[20]

1. For the purposes of this Article, an emergency means a situation in which there is a significant and imminent risk to the life or safety of any natural person.

2. 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.

3. A requested Party shall accept such request in electronic form. However, it may require appropriate levels of security and authentication before accepting the request.

4. 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 the most rapidly expedited basis possible.

5. Once satisfied that an emergency exists and the other requirements for mutual assistance are satisfied, the requested Party shall respond to the request on the most rapidly expedited basis possible.

6. Each Party shall ensure that a person from its authority responsible for responding to mutual assistance requests under Article 25 or 27 of the Convention is available on a twenty-four hour, seven-day-a-week basis for purposes of responding to a request under this Article.

7. The authorities responsible for mutual assistance of the requesting and requested Parties responsible for mutual assistance may agree to provide 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 an alternate channel other than that used for the request.

8. a. In the event of an emergency, requests may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party, or through Interpol or the 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 the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

[19] Text as agreed provisionally by the PDP, Strasbourg, 11 July 2018. Text may change as the Protocol evolves and comments are received.

[20] ***To be added in the Protocol:

- for the purposes of this Article, the scope of mutual assistance shall be identical to that set forth in Article 25 of the Budapest Convention.
- for greater certainty, nothing in this article prevents the sharing of information or the provision of other international assistance through other available avenues of international cooperation.
- this provision does not exclude other options [E.g. "This provision does not preclude the voluntary transmission of data to foreign competent authorities by internet service providers in conformity with their domestic and international applicable rules ".]

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

8.2 Draft Explanatory Report

1. Protocol Article [Emergency mutual assistance] is intended to provide a maximally expedited procedure for mutual assistance requests made in emergency situations. An emergency is defined in paragraph 1 as being those in which there is a significant and imminent risk to the life or safety of a natural person. The definition is intended to cover situations in which the risk is imminent, meaning that it does not include situations in which the risk to the life or safety of the person has already passed, or in which there may be a future risk that is not imminent. The reason for this very precise definition is that the article places labor 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.

2. Because protocol Article [ ] is limited to the circumstances justifying such rapidly accelerated action, it is distinct from Article 25(3) of the main 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(3) is broader in scope than protocol Article [ ], in that 25(3) covers situations not covered in Article [ ], 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(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 [ ] are significantly greater; i.e. where MLA is required to prevent significant and imminent risk to life or safety, the process should be even more accelerated. Emergencies involving a significant and imminent risk to the life or safety of a person often involve hostage situations in which there is a credible risk of imminent loss of life, serious injury or other harm to the victim and the suspect is negotiating for ransom via email or social media so that the location of the victim may be determined through data stored by the provider, sexual abuse of a child as evidenced by the discovery of recently produced child sexual exploitation or child sexual abuse materials, or other indicia of abuse, 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 of danger to life or safety of a natural person.

3. Under paragraph 2, in making an emergency request, the requesting Party must both conclude that an emergency within the meaning of the article 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(4) of the Convention, execution of requests for mutual assistance, including emergency requests, 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".

4. Paragraph 3 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.

5. Where the requested Party requires additional information to come to the conclusion that there is an emergency within the meaning of paragraph 1, and/or that the other requirements for mutual assistance have been met, it is required by paragraph 4 to seek the additional information as rapidly as possible. Conversely, paragraph 4 requires the requesting Party to provide the supplemental information in the same rapidly expedited manner. Both Parties are thus required to do their utmost to avoid loss of time that could inadvertently contribute to a tragic result.

6. Under paragraph 5, once the needed information has been provided to enable the request to be executed, the requested Party is required to use the same maximally accelerated efforts to do so. This generally means rapidly expediting the obtaining of judicial orders compelling a provider to produce data that is evidence of the offense 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 State, however.

7. Under paragraph 6, all Parties shall ensure that members of its central authority for mutual assistance (or, if Article [ ](8) is applicable, the relevant judicial authorities concerned) 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 authority responsible for responding to mutual assistance requests under Article 25 or 27 of the Convention to be staffed and operational 24/7. Rather, that authority should implement procedures to ensure that staff may be contacted in order to review emergency requests outside normal business hours.

8. Paragraph 7 provides a basis for the Parties concerned to agree upon an alternate channel for transmission of the responsive evidence or information, 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 evidence or information provided in [the] execution of the requesting Party's request, they may agree to use a different channel to speed transmission, maintain the integrity of the evidence, or other reason. For example, in an emergency, the Parties may agree to 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 Parties may also agree, 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 the transmission of sensitive evidence.

9. Finally, paragraph 8 is a more compressed version of Article 27(9) of the main Convention, by which Parties to the protocol can provide for requests to be made directly between 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 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 the central authority for mutual assistance could be counter-productive in that, without guidance and/or approval from the central authority, the receiving authority may not be empowered to act independently, or may not be familiar with the proper procedure. Therefore, as in Article 25(9)(e), each Party may notify the Council of Europe Secretary General that requests under this Article must be addressed only to its central authority.