EUROPEAN
COMMISSION

Brussels, 5.2.2019
COM(2019) 71 final

Recommendation for a

COUNCIL DECISION

authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185)

EXPLANATORY MEMORANDUM

1. CONTEXT

The evolution of information and communication technologies – while bringing unprecedented opportunities for mankind – also raises challenges, including for criminal justice and thus for the rule of law in cyberspace. While cybercrime and other offences entailing electronic evidence on computer systems are thriving and while evidence relating to these offences is increasingly stored on servers in foreign, multiple, shifting or unknown jurisdictions, that is, in the cloud, the powers of law enforcement remain limited by territorial boundaries.

The European Commission committed in the April 2015 European Agenda of Security[1] to review obstacles to criminal investigations into cyber-enabled crimes, notably on cross-border access to electronic evidence. On 17 April 2018, the Commission proposed to the Council and the European Parliament a Regulation on European Production and Preservation orders for electronic evidence in criminal matters[2] and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings ("e-evidence proposals")[3]. The purpose of these proposals is to speed up the process in the European Union to secure and obtain electronic evidence that is stored and/or held by service providers established in another jurisdiction.

The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime (CETS No. 185) aims at facilitating the fight against criminal offences making use of computer networks. It contains provisions (1) harmonising domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime, (2) provides for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form, and (3) aims to set up a fast and effective regime of international cooperation. The Convention is open to Member States of the Council of Europe and non-members. 62 countries are currently Parties to the Convention, including 26 European Union Member States[4]. The Convention does not envisage that the European Union may accede to the Convention. The European Union is nevertheless recognised as an Observer Organisation to the Convention Committee (T-CY). On that basis the European Union takes part in meetings of the Convention Committee.

Article 46.1.c of the Convention provides that the Parties shall, as appropriate, consult periodically with a view to facilitating consideration of possible supplementation or amendment of the Convention. The Parties to the Convention on Cybercrime have been looking for some time now into existing challenges and obstacles to access by national judicial and police authorities to electronic evidence of crimes under criminal investigation in

---

1 Communication from the Commission to the European Parliament and Council: The European Agenda on Security, 28 April 2015, COM(2015) 185 final.

2 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM(2018) 225 final

3 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, COM(2018) 226 final.

4 All except Ireland and Sweden, which have signed but not ratified the Convention, but nevertheless committed to pursuing accession.

form of computer data, that is from 2012 to 2014 through a working group on transborder access to data and from 2015 to 2017 through the Cloud Evidence Group.

Negotiations for a Second Additional Protocol to the Convention

After proposals from the Cloud Evidence Group[5], the Cybercrime Convention Committee (T-CY) adopted several Recommendations, including on the negotiation of a Second Additional Protocol to the Convention on Cybercrime[6] on enhanced international cooperation ('Second Additional Protocol'). In June 2017, the Cybercrime Convention Committee approved the Terms of Reference for the preparation of the Second Additional Protocol during the period from September 2017 to December 2019.

In accordance with the Terms of Reference, the Second Additional Protocol may include the following elements:

- Provisions for more effective mutual legal assistance, in particular:
  - a simplified regime for mutual legal assistance requests for subscriber information;
  - international production orders;
  - direct cooperation between judicial authorities in mutual legal assistance requests;
  - joint investigations and joint investigation teams;
  - requests in English language;
  - audio/video hearing of witnesses, victims and experts;
  - emergency Mutual Legal Assistance (MLA) procedures;
- Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests;
- Clearer framework and stronger safeguards for existing practices of transborder access to data;
- Safeguards, including data protection requirements.

Negotiations of different provisions of the Second Additional Protocol are progressing at different speeds. The current situation in the working groups on the four main blocks of work outlined in the terms of reference are as follows:

- Provisions on "Languages of requests" and "Emergency mutual assistance" were preliminarily adopted by the Protocol Drafting Plenary in July 2018.
- Provisions on "Video conferencing" were preliminarily adopted by the Protocol Drafting Plenary in November 2018.
- The Protocol Drafting Plenary in November 2018 also allowed for detailed discussions (provisions on "Jurisdiction" and "Endorsement model") and updates

5 Final report of the T-CY Cloud Evidence Group 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY' of 16 September 2016.

6 The first additional protocol (CETS No. 189) to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems was open for signature by the States, which have signed the Convention in 2003. 31 countries are parties to the first additional protocol, including 17 EU Member States.

("Direct cooperation with providers", "International production orders", "Extending searches/access based on credentials", "Joint investigations and joint investigation teams" and "Investigative techniques").

- Sufficient progress has not yet been made on other issues (safeguards, including data protection requirements).

2. OBJECTIVES OF THE PROPOSAL

This recommendation is submitted to the Council in order to receive authorisation to participate in negotiations on behalf of the European Union and its Member States on a Second Additional Protocol, to adopt negotiating directives and to appoint the Commission as negotiator in accordance with the draft negotiating directives attached, pursuant to Article 218 TFEU.

Article 3(2) TFEU provides that the Union has exclusive competence "*for the conclusion of an international agreement ... in so far as its conclusion may affect common rules or alter their scope*." An international agreement may affect common rules or alter their scope where the area covered by the agreement overlaps with Union legislation or is covered to a large extent by Union law.

The European Union has adopted common rules based on Article 82(1) and 16 TFEU on elements being considered for the Second Additional Protocol. The current European Union legal framework includes in particular instruments on law enforcement and judicial cooperation in criminal matters, such as the Directive 2014/41/EU regarding the European Investigation Order in criminal matters[7], the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[8], Regulation 2018/1727 on Eurojust[9], Regulation 2016/794 on Europol[10], Council Framework Decision 2002/465/JHA on joint investigation teams[11], Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings[12]. Moreover, the Union has adopted several directives that reinforce procedural rights of suspects and accused persons[13].

---

7 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, p.1.

8 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C197, 12.7.2000, p.1.

9 Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA.

10 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53.

11 Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams, OJ L 162, 20.6.2002, p. 1.

12 Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, OJ L328, 15.12.2009, p.42;

13 Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ L 280, 26.10.2010, p. 1; Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, p. 1; Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of

Externally, the European Union has concluded a number of bilateral agreements between the Union and third countries, such as the Agreements on Mutual Legal Assistance between the European Union and the United States of America[14] and between the European Union and Japan[15].

The protection of personal data is a fundamental right enshrined in EU Treaties and in the Charter of Fundamental Rights of the European Union and personal data may only be processed in accordance with the Regulation (EU) 2016/679 (the General Data Protection Regulation)[16] and Directive (EU) 2016/680 (the Police Data Protection Directive)[17]. The fundamental right of everyone to the respect for his or her private and family life, home and communications is also enshrined in the Charter of Fundamental Rights, and includes the respect for the privacy of one's communications as an essential element. Electronic communications data can only be processed in accordance with Directive 2002/58/EC (the ePrivacy Directive)[18].

Moreover, to assess whether an area is largely covered by common rules account must be taken not only of Union law as it currently stands in the area concerned, but also of its future development, in so far as that is foreseeable at the time of that analysis. The area covered by the Second Additional Protocol is of direct relevance to foreseeable future developments of the relevant common rules. In this respect, the Commission's April 2018 proposals on cross-border access to electronicevidence are also relevant.[19]

---

liberty, OJ L 294, 6.11.2013, p. 1; Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, p. 1; Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132, 21.5.2016, p. 1; Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, p. 1; Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings.

14 Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11.2009, p. 40–41.

15 Agreement between the European Union and Japan on mutual legal assistance in criminal matters, OJ L 39, 12.2.2010, p 20.

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

17 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

18 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37), amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

19 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM(2018) 225 final; Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, COM (2018) 226 final.

The scope of the proposals includes specific types of service providers that are providing services in the European Union. A provider is offering services in the European Union when it enables users in one or more Member States to use its services and where it has a substantial connection to the Union, for instance when it has an establishment in a Member State or because it provides services to a large number of users in that Member State. Those without a presence in the European Union are obliged to appoint a legal representative against whom production orders can be enforced.

The European Council Conclusions of 18 October state that "*Solutions should be found to ensure swift and efficient cross-border access to e-evidence in order to effectively fight terrorism and other serious and organised crime, both within the EU and at international level; the Commission proposals on e-evidence and access to financial information, as well as to better combat money laundering, should be agreed on by the end of the legislature. The Commission should also urgently submit negotiating mandates for the international negotiations on e-evidence*".

The Commission's e-evidence proposals provide the basis for a coordinated and coherent approach both within the European Union and by the European Union at international level, with due regard to European Union rules, including on non-discrimination between European Union Member States and their nationals. While the Commission, in its Impact Assessment for the e-evidence proposals, already noted that the proposals could usefully be complemented by bilateral or multilateral agreements on cross-border access to electronic evidence with accompanying safeguards, the Commission decided to propose EU rules on the appropriate modalities and safeguards for cross-border access to electronic evidence, before engaging in international negotiations with third parties.[20]

At the international level, the Commission has continued to participate as observer in related discussions within the framework of the Council of Europe Convention on Cybercrime[21]. Cross-border access to electronic evidence has been a regular point on recent EU-US Justice and Home Affairs Ministerial meetings.

The two recommendations to participate in the negotiations of the Second Additional Protocol to the Convention on Cybercrime and to open negotiations with the United States of America are being adopted by the Commission at the same time. While the two processes will progress at a different pace, they address inter-linked issues and commitments taken in one negotiation may have a direct impact on other strands of negotiations.

While the e-evidence proposals address the situation of specific types of service providers providing services on the EU market, there is a risk of conflicting obligations with laws in third countries. In order to address these conflicts of law, and in line with the principle of international comity, the e-evidence proposals include provisions for specific mechanisms in case a service provider is confronted with conflicting obligations deriving from the law of a third country when evidence is requested. These mechanisms include a review procedure to clarify such a situation. The Second Additional Protocol to the Council for Europe Convention on Cybercrime should aim to avoid conflicting obligations between the Parties to the Convention on Cybercrime.

It can therefore be considered that the conclusion of the Second Additional Protocol may affect common rules or alter their scope.

---

[20] While negotiations with the European Parliament and the Council are ongoing, the Council agreed a general approach on the Commission proposal for a Regulation at the Justice and Home Affairs Council on 7 December 2018.

[21] Council of Europe Budapest Convention on Cybercrime (CETS N° 185), 23 November 2001, http://conventions.coe.int.

The Union accordingly has exclusive competence for the negotiation of the Second Additional Protocol supplementing the Convention on Cybercrime (by virtue of Article 3(2) TFEU).

The subject matter of the Second Additional Protocol would fall within EU policies and competences, in particular in the field of instruments on judicial cooperation in criminal matters (Article 82(1) TFEU) and data protection (16 TFEU) and, as a matter of EU law, negotiations could not be conducted without EU participation. Moreover, the Commission has a general role in representing the European Union provided for in Article 17(1) TEU. In view of the above, the Commission should be appointed by the Council as the negotiator for the Second Additional Protocol supplementing the Convention on Cybercrime (CETS No. 185).

3. RELEVANT PROVISIONS IN THE POLICY AREA

The negotiations should ensure that the agreed provisions are compatible with EU law and Member States' obligations under it, taking also account of its future development. Moreover, it will also be necessary to ensure that the Second Additional Protocol will include a disconnection clause allowing the European Union Member States that become Parties to the Second Additional Protocol to regulate the relations among themselves on the basis of EU law. In particular, the functioning of the European Commission's e-evidence proposals, including as they evolve in the legislative procedure negotiations by the co-legislators and eventually in their final (adopted) form, should be preserved amongst European Union Member States.

The Second Additional Protocol should include the necessary safeguards for fundamental rights and freedoms recognised by the Charter of Fundamental rights of the European Union, in particular the right to private and family life, home and communications recognised in article 7 of the Charter, the right to protection of personal data recognised in Article 8 of the Charter, the right to effective remedy and fair trial recognised in Article 47 of the Charter, the presumption of innocence and right of defence recognised in Article 48 of the Charter and principles of legality and proportionality of criminal offences and penalties recognised in Article 49 of the Charter. The Second Additional Protocol should be applied in accordance with those rights and principles.

Appropriate data protection and privacy safeguards for the collection, transfer and subsequent use of personal data and electronic communications data must be part of the protocol so as to ensure full compliance by EU service providers with their obligations under EU data protection and privacy laws, insofar as such an international agreement could provide a legal basis for data transfers in reaction to production orders or requests issued by an authority from a non-EU Party to the Additional Protocol requiring a controller or processor to disclose personal data and electronic communications data. They should thus ensure the protection of fundamental rights and freedoms of EU citizens, including privacy and personal data protection when personal data or electronic communications data is disclosed to law enforcement authorities in countries outside the European Union.

In view of the absence of provisions for authorities to access data without the help of an intermediary ('direct access') in the European Commission's e-evidence proposals, any use of those measures can only be based on national law. Where the Second Additional Protocol may include provisions in relation to the 'Extension of searches and access based on credentials' and 'Investigative Techniques', the main aim should be to pursue stronger safeguards for such cross-border direct access to data to ensure the protection of fundamental rights and freedoms of EU citizens, including privacy and personal data protection.

The conclusion of the Second Additional Protocol should allow for the conclusion of bilateral agreements or treaties between the Parties to the Protocol and between the Parties of the Protocol and the European Union, governing their relations. To this end, an appropriate clause should be inserted envisaging that if two or more Parties to the Convention have already concluded an agreement or treaty on the matters dealt with in the Convention, or should they in future do so, they are entitled to apply that agreement or treaty or to regulate those relations accordingly, provided that this is done in a manner that is consistent with the Convention's objectives and principles. The agreement between the European Union and the United States on cross-border access to electronic evidence for judicial cooperation in criminal matters should, in the bilateral relations between the United States of America and the European Union, take precedence over any agreement or arrangement reached in the negotiations of the Second Additional Protocol, in so far as it covers the same issues.

Recommendation for a

COUNCIL DECISION

authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 218(3) and (4) thereof,

Having regard to the recommendation from the European Commission,

Whereas:

(1) On 9 June 2017, the Committee of Parties to the Council of Europe Convention on Cybercrime (CETS No. 185) (T-CY) adopted a decision adopting the Terms of Reference for the preparation of a Second Additional Protocol to the Convention.

(2) The Terms of Reference for the Second Additional Protocol include the following elements for reflection: provisions for more effective mutual legal assistance (a simplified regime for mutual legal assistance requests for subscriber information; international production orders; direct cooperation between judicial authorities in mutual legal assistance requests; joint investigations and joint investigation teams; requests in English language; audio/video hearing of witnesses, victims and experts; emergency Mutual Legal Assistance procedures); provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests; clearer framework and stronger safeguards for existing practices of transborder access to data; safeguards, including data protection requirements.

(3) The Union has adopted common rules that overlap to a large extent with the envisaged elements being considered for the Second Additional Protocol. This includes in particular a comprehensive set of instruments in order to facilitate judicial cooperation in criminal matters,[22] to ensure minimum standards of procedural rights[23], as well as data protection and privacy safeguards[24].

---

22 Council Act of 29.5.2000 establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C197, 12.7.2000, p.1; Regulation (EU) 2018/1727 of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018; Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53; Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams, OJ L 162, 20.6.2002, p. 1; Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, OJ L328, 15.12.2009, p.42; Directive 2014/41/EU regarding the European Investigation Order in criminal matters, OJ L130, 1.5.2014, p.1.

23 Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ L 280, 26.10.2010, p. 1; Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, p. 1; Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in

(4) The Commission also submitted legislative proposals for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, and for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings introducing, binding cross-border European Production and Preservation Orders to be addressed directly to a representative of a service provider in another Member State[25].

(5) Therefore, the Second Additional Protocol may affect common Union rules or alter their scope.

(6) Articles 82(1) and 16 of the Treaty on the Functioning of the Union specify Union competencies in the area of judicial cooperation in criminal matters as well as in data protection and privacy. In order to protect the integrity of Union law and to ensure that the rules of international law and Union law remain consistent, it is necessary that the Union participates in the negotiations on the Second Additional Protocol.

(7) The Second Additional Protocol should include the necessary safeguards for fundamental rights and freedoms, including the right in protection of personal data and privacy, the right to private and family life, home and communications recognised in article 7 of the Charter, the right to protection of personal data recognised in Article 8 of the Charter, the right to effective remedy and fair trial recognised in Article 47 of the Charter, the presumption of innocence and right of defence recognised in Article 48 of the Charter and principles of legality and proportionality of criminal offences and penalties recognised in Article 49 of the Charter. The Second Additional Protocol should be applied in accordance with those rights and principles.

(8) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[26] and delivered an opinion on …[27],

HAS ADOPTED THIS DECISION:

Article 1

The Commission is hereby authorised to negotiate, on behalf of the Union, the Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185).

European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, p. 1; Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, p. 1; Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132, 21.5.2016, p. 1.

24 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

25 COM (2018) 225 final and COM (2018) 226 final.

26 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L295, 21.11.2018, p. 39).

27 OJ C ...

Article 2

The negotiating directives are set out in the Annex.

Article 3

The negotiations shall be conducted in consultation with a special committee to be designated by the Council.

Article 4

This Decision is addressed to the Commission.

Done at Brussels,

For the Council
The President

EUROPEAN
COMMISSION

Brussels, 5.2.2019
COM(2019) 71 final

ANNEX

ANNEX

to

the Recommendation for a COUNCIL DECISION

authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185)

ANNEX

1. OBJECTIVES

The Commission should, in the course of the negotiations, aim to achieve the objectives set out in detail below:

(a) The negotiations should ensure full compatibility of the Convention and the Additional Protocols with EU law and Member States' obligations under it, in particular as regards investigatory powers granted to non-EU Parties.

(b) In particular, the negotiations should ensure respect for the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and Charter of Fundamental Rights, including proportionality, procedural rights, the presumption of innocence and the rights of defence of persons subject to criminal proceedings as well as privacy and the protection of personal data and electronic communications data when such data is processed, including transfers to law enforcement authorities in countries outside the European Union, and any obligations incumbent on law enforcement and judicial authorities in this respect.

(c) Furthermore, the Second Additional Protocol should be compatible with the Commission's e-evidence legislative proposals, including as they evolve in the legislative procedure negotiations by the co-legislators and eventually in their final (adopted) form, and prevent conflicts of laws. In particular, such a protocol should to the greatest extent possible reduce the risks of production orders issued under a future EU instrument creating conflicts with the laws of third countries that are Parties to the Second Additional Protocol. When accompanied by appropriate data protection and privacy safeguards, it would facilitate compliance by EU service providers with their obligations under EU data protection and privacy laws, insofar as such an international agreement could provide a legal basis for data transfers in reaction to production orders or requests issued by an authority from a non-EU Party to the Second Additional Protocol requiring a controller or processor to disclose personal data or electronic communications data.

2. SPECIFIC ISSUES

I. Relation with EU law and other (possible) agreements

(d) It should be ensured that the Second Additional Protocol contains a disconnection clause providing that the Member States shall, in their mutual relations, continue to apply the rules of the European Union rather than the Second Additional Protocol.

(e) The Second Additional Protocol may apply in the absence of other more specific international agreements binding the European Union or its Member States and other Parties to the Convention, or, where such international agreements exist, only to the extent that certain issues are not regulated by those agreements. Such more specific international agreements should thus take precedence over the Second Additional Protocol provided that they are consistent with the Convention's objectives and principles.

II. Provisions for more effective mutual legal assistance:

(f) The provisions on the 'languages of requests' as currently drafted stipulate that requests should be made in a language acceptable to the requested Party or

accompanied by a translation into such a language. The European Union should support the draft text and explanatory report preliminarily adopted.

(g) The provisions on the 'emergency mutual assistance' as currently drafted enable mutual assistance to be sought on a rapidly expedited basis by sending such a request in electronic form where the requesting Party is of the view that an emergency exists, defined as a situation in which there is a significant and imminent risk to the life or safety of any natural person. The European Union should support the draft text and explanatory report preliminarily adopted. The scope of mutual assistance should be identical to that set forth in Article 25 of the Convention.

(h) With regard to the provisions on 'video conferencing' the European Union should seek that the Second Additional Protocol is consistent with the corresponding provisions of the existing international agreements between European Union and its Member States and other Parties to the Convention, where possible. The provisions should allow Member States to ensure the respect of applicable procedural rights safeguards deriving from Union and national law.

(i) With regard to the provisions on 'endorsement model' the European Union should seek that the draft text and explanatory memorandum include elements, such as mandatory maximum deadlines for decisions by national authorities, to ensure that its use results in swifter procedures; further, it should ensure that the burden on service providers is proportionate, and the remedies, where appropriate, shall apply;

III. Provisions allowing for direct cooperation with service providers in other jurisdictions:

(j) With regard to the provisions on 'direct cooperation with providers across jurisdictions', the European Union should ensure that the Second Additional Protocol is consistent with EU law, includes the appropriate safeguards and the burden on service providers is proportionate.

(k) With regard to the provisions on 'International productions orders', the European Union should ensure that the Second Additional Protocol includes appropriate fundamental rights safeguards, taking into account the different level of sensitivity of the categories of data concerned and the safeguards included in the European Production Orders for the different categories of data.

(l) With regard to the provisions on 'International productions orders', the European Union should not oppose the inclusion in the Second Additional Protocol of additional safeguards and grounds for refusal compared to the Commission's e-evidence proposals, including as they evolve in the legislative procedure negotiations by the co-legislators and eventually in their final (adopted) form, such as a notification and consent by the state of the service provider and a prior review carried out either by a court or by an independent administrative body, as far as this does not disproportionately reduce the effectiveness of the instrument under the Second Additional Protocol (for example in cases of validly established urgency). Any additional safeguards and grounds for refusal should not affect the functioning of the EU's e-evidence proposals amongst Member States.

IV. Stronger safeguards for existing practices of transborder access to data:

(m) With regard to the provisions on 'Extension of searches and access based on credentials' and 'Investigative Techniques', the European Union should ensure that

the Second Additional Protocol includes appropriate fundamental rights safeguards. Therefore, the draft text should also include the condition that the data stored in the connected computer system is lawfully accessible from the initial system and the access is necessary and proportionate and does not involve a breach of security measures in devices in line with the safeguards outlined below.

(n) The European Union should also ensure that it does not restrict the possibilities for such access that are currently provided for in Member States.

V. Safeguards, including data protection requirements:

(o) The European Union should ensure that the Second Additional Protocol provides for appropriate data protection safeguards within the meaning of Directive (EU) 2016/680 and Regulation (EU) 2016/679 and Directive 2002/58/EC for the collection, transfer and subsequent use of personal data and electronic communications data included in the electronic evidence sought by the requesting authority. These safeguards should be included in the Second Additional Protocol, taking into account those set out in EU agreements, such as the EU-US Umbrella Agreement and in the modernised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data(CETS No.108). These safeguards should address situations of processing of data in the context of both mutual assistance between law enforcement authorities and direct cooperation between law enforcement authorities and providers. The European Union should aim for these safeguards to apply to all investigatory powers, both existing in the context of the Convention and created by the Second Additional Protocol.

3. TERRITORIAL APPLICATION, ENTRY INTO FORCE AND OTHER FINAL PROVISIONS

The final provisions of the Additional Protocol, including provisions on entry into force, reservations, denunciation etc. should be modelled where possible and appropriate along the provisions of the Council of Europe Convention on Cybercrime (CETS No.185). Provisions diverging from standard clauses should only be used where necessary to obtain the objectives or to reflect the specific circumstances of the Second Additional Protocol.