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.