EUROPEAN
COMMISSION

Brussels, 29.3.2022
COM(2022) 132 final

ANNEX

ANNEX

to the

Recommendation for a Council Decision

authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes

ANNEX

Regarding the process of the negotiations, the Union should aim to achieve that:

(1) The negotiation process is open, inclusive and transparent, and based on cooperation in good faith.

(2) The negotiation process enables participation in a meaningful way of all relevant stakeholders, including civil society, the private sector, academia and non-governmental organisations.

(3) All the inputs received from the entire United Nations Membership are considered on an equal basis to ensure an inclusive process.

(4) The negotiation process is based on an effective and realistic work programme.

Regarding the general objectives for the negotiations, the Union should aim to achieve that:

(5) The Convention serves as an effective instrument for criminal law enforcement and judicial authorities in the global fight against cybercrime, with the aim to add value to international cooperation.

(6) The existing framework of tried-and-tested international and regional instruments and efforts as reflected in United Nations General Assembly Resolutions 74/247 and 75/282 is taken into full consideration. Accordingly, the Convention is compatible with and complement existing international instruments, in particular the 2001 Council of Europe Budapest Convention on Cybercrime and its protocols, the 2000 United Nations Convention against Transnational Organized Crime and its protocols, but also other relevant international and regional instruments. The Convention avoids any impact on their application or the further accession of any country to them and, to the extent possible, avoid unnecessary duplication.

(7) The work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime as agreed by United Nations General Assembly Resolution 75/282 are taken into full consideration.

(8) The provisions of the Convention achieve the highest possible protection of human rights. EU Member States should be able to comply with EU law, including the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter of Fundamental Rights. The provisions of the Convention should also be compatible with the EU's and its Member States' international trade obligations.

Regarding the substance of the negotiations, the Union should aim to achieve that:

(9) The Convention provides for definitions of offences that can only be committed using information systems.

(10) The Convention provides for definitions of offences that can be committed without using information systems but that can be enabled by the use of information systems in certain circumstances, but only in cases where the involvement of information systems substantially changes the characteristics or impact of the offences.

(11) The offences are clearly and narrowly defined in a technology neutral manner. The definitions are compatible with those in other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and with international human rights standards.

(12) The Convention provides for rules on the attempt, aiding and abetting of such offences, on the liability of legal persons for such offences, for rules on the establishment of jurisdiction over such offences, and on sanctions and measures in relation to such offences that are compatible with other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and with international human rights standards.

(13) The Convention provides for procedural criminal measures that allow authorities to investigate cybercrimes effectively, to freeze and confiscate proceeds of such crimes and to preserve or obtain electronic evidence of any criminal offence as part of a criminal investigation or proceeding, taking due account of the proportionality principle.

(14) Those procedural criminal measures provide sufficient added value compared to other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and are compatible with such conventions and with international human rights standards.

(15) Procedural measures to preserve or obtain electronic evidence contain a clear and narrow definition of the type of information covered. Procedural measures for cooperation with private sector entities ensure that the burden on such entities is proportionate and that private sector entities fully respect the human rights of their users. The Convention provides legal clarity for online service providers (e.g., Internet service providers) in their interactions with law enforcement authorities of the State Parties to the Convention. Procedural measures for the removal of illegal content only relate to illegal content that can be sufficiently specific and narrowly defined.

(16) The Convention provides for cooperation measures that allow authorities in different States that are party to the instrument to cooperate effectively for the purpose of criminal investigations or proceedings concerning offences defined in the instrument or to cooperate to preserve or obtain electronic evidence of any criminal offence as part of a criminal investigation or proceeding.

(17) Those cooperation measures provide sufficient added value compared to other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and are compatible with such conventions and with international human rights standards.

(18) Cooperation measures are subject to the conditions provided for by the law of the requested Party and provide for broad grounds for refusal such as to ensure the protection of fundamental rights, including the right to the protection of personal data, including in the context of personal data transfers, and, where appropriate, the existence of double criminality.

(19) The Convention provides for strict conditions and strong safeguards to ensure that EU Member States can respect and protect the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter of Fundamental Rights, including, in particular, the principle of proportionality, procedural guarantees and rights, the right to effective judicial

redress, the presumption of innocence, the right to a fair trial, and the rights of defence of persons subject to criminal proceedings, as well as the right to privacy, the right to the protection of personal data and of electronic communications data when such data is processed, including for transfers to authorities in countries outside the European Union, and the right to freedom of expression and information. The Convention ensures in particular that EU Member States are able to comply with requirements for the international transfers of personal data within the meaning of Directive (EU) 2016/680, Regulation (EU) 2016/679 and Directive 2002/58/EC. The conditions and safeguards also ensure the protection of human rights and fundamental freedoms in line with international human rights standards. This applies to the entire Convention, including procedural measures and cooperation measures, including those that may significantly interfere with individuals' rights, such as the freezing and confiscation of proceeds of crime and extradition.

(20) The Convention provides a basis for voluntary capacity building measures to support countries in their ability to conduct effective cybercrime investigations and proceedings and to obtain electronic evidence for investigations and proceedings of other offences, including by means of technical assistance and training. The UNODC has a clearly described role for the implementation of such measures.

(21) The Convention takes due account of the position of natural and legal persons as victims of cybercrime. The Convention ensures that these victims of cybercrime receive appropriate assistance, support and protection.

(22) The Convention provides a basis for practical measures for the prevention of cybercrime that are clearly defined and strictly limited and distinct from criminal procedural measures that could interfere with the rights and freedoms of individuals or legal persons.

Regarding the functioning of the Convention, the Union should aim to achieve that:

(23) The Convention preserves existing global and regional instruments and ongoing international cooperation in the global fight against cybercrime. In particular, the European Union Member States, in their mutual relations, are able to continue to apply the rules of the European Union.

(24) The Convention provides for an appropriate mechanism to ensure its implementation and provide for final provisions, including on the settlement of disputes, signature, ratification, acceptance, approval and accession, entry into force, amendment, suspension, denunciation and depositary and languages that are modelled where possible and appropriate along the provisions of other relevant international or regional conventions in particular in the area of organised crime or cybercrime.

(25) The Convention allows for the European Union to become a party to it.