Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

(Draft Protocol version 2)

By communication of April 15, 2021, the Secretariat of the T-CY invited stakeholder to comment by 2 May on the draft text of the Second Additional Protocol to the Budapest Convention, approved by the T-CY Protocol Drafting Plenary on 12 April. Following this invitation, the European Union Agency for Fundamental Rights ('FRA') would like to take the opportunity to provide its comments on the draft.

FRA comments

FRA welcomes the draft of the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, as well as the possibility to comment thereon.

The draft replies to the need to establish a clear, foreseeable, and operational legal framework, supporting both international cooperation on cybercrime and the collection of e-evidence related to a criminal offence for criminal investigations and proceedings. The draft Second Additional Protocol sets up legal boundaries, paying specific attention to fundamental tights, and notably to the right to the protection of personal data.

In a view of further reinforcing the legal clarity and foreseeability of the text, FRA suggests the following points to be considered. FRA believes that, through the following suggestions, the protection of Fundamental Rights could be reinforced.

- Art. 11 (1) in conjunction with Art. 11 (5): The *ne bis in idem* principle could be reflected in the Protocol to avoid double penalization of the witness in case of a false statement or perjury/false oath, if both states administered the oaths, warnings and instructions.
- Art. 11 (7): If video conferencing technology is generally permitted by the Protocol, it should also accommodate witness protection measures available at national level, such as e.g. face or voice distortion.

FRA further welcomes the draft of the Second Additional Protocol for allowing prior prosecutorial, judicial and/or independent authorisation and supervision of the orders foreseen in Art. 7 (2) (b) and Art. 8, providing the opportunity to protect fundamental rights and avoid abuse and excessive use. Mindful that, in the absence of such safeguards, unwanted fundamental rights implications might occur, the Agency suggests to EU Member States to ensure such safeguards when depositing their instruments of ratification, acceptance or approval and transposing the Protocol into national law.

In addition, FRA believes that in some instances, further guidance or clarification could be added to the additional protocol, to strengthen the legal clarity and foreseeability of the text.

- Art. 3 (2): A "significant and imminent risk" could be further delineated, to prevent abuse or excessive use of cross-border expedited production orders. In addition, the criteria under which a person is either "identified" or "identifiable" could be more clearly stated, to provide legal clarity and foreseeability.
- Art. 6 (2) and (3): Similarly, further guidance on what constitutes "reasonable conditions", as well as further criteria setting out under which circumstances "*relevance to a specific criminal investigation or proceeding*" is given, could prove useful, not only from a rights perspective, but also considering operationality and cross-border cooperation.

- Arts. 7, 8 in conjunction with Art. 18 (1) of the Cybercrime Convention: "*Subscriber information*" is not defined solely for the purposes of the protocol, could be understood broadly, and not be limited to data necessary in investigations and proceedings. For that reason, the term could be further defined to encompass only information and data that are necessary in criminal investigations and proceedings. This would comply with the principles of data minimisation and purpose limitation.
- Art. 7 (1); Art. 8(1): These articles foresee competent authorities to request the data by means of an order. Equality of arms would require that the defence has the same possibilities. For that reason, it could be foreseen that, at national level, upon request, Contracting Parties' competent authorities also act on behalf of the defence. In addition, the circumstances under which "*information is needed for the issuing Party's specific criminal investigations or proceedings*" could be clarified, to avoid abuse and excessive use.
- Arts. 7 (7) and (8), and 8: To enhance legal clarity and foreseeability, the reasons for which a service provider may lawfully refuse to disclose subscriber information could be provided. Violations of fundamental rights in the requesting or requested state should be such a reason. In addition, some criteria supporting a "*reasonable explanation"* could be listed in a non-exhaustive manner.
- In Art. 8 (3) (b) (v), Art. 9 (3) (e); Art. 10 (1): Further guidance could be provided to ensure respect for the presumption of innocence.
- Art. 14 (4): Further guidance as to the safeguards against the risk of unwarranted prejudicial impact from the use of sensitive data could be provided, to prevent abuse and unwanted fundamental rights implications.
- Art. 14 (5): The retention periods could be defined further, clarifying:
    - whether the data should be kept until an investigation is concluded, until a judgment is delivered, until a judgment is final or until a sentence is served;
    - when a "proceeding" is to be considered finished; and
    - for how long after such proceedings and for what particular reasons the data shall be kept.
- Art. 14 (7) (a): Further guidance could be provided as to the particular measures and the question of what makes the required measures appropriate, considering that fundamental rights are concerned.
- Art. 14 (8): Further guidance concerning the records to be maintained could also be considered. This guidance could clarify to what personal data these records should be limited and when and under which circumstances (maintained) records will be deleted.