ESTONIA

Firstly, Estonia wants to thank the Portuguese Presidency for the constructive session regarding the Europol regulation amendments.

Estonia presents the following comments:

Data and private sector

1) **Article 4(1)(m) -** We welcome the inclusion of the provision, particularily in light of the need to coordinate MS actions under the TCO regulation.

2) **Article 4(1)(u)** – as discussed, the term 'crisis situation' is not defined in EU legal landscape and every MS understands this differently. Crisis situation depends on a variety of things and may be seen differently by the MSs. Therefore we ask, whether this term is needed here. Firstly, it doesn't matter if there is 1 victim or more, or if there was just an attempt. Disinformation spreads nevertheless. Secondly, Crisis Protocol aims to provide a "rapid response to contain the viral spread of terrorist and violent extremist content online"[1]. Therefore crisis refers more to the scope of information than a specific event.

Secondly, there is an explanation "depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population". In our opinion, each real life event based on which a certain online content campaign may be launched, qualifies into that description. **In short: to avoid confusion and unclarity, our proposal is to discuss the potential removal of this term.** In this regard, Estonia sees, that (u) could be further capped as following:

"(u) support Member States' actions in preventing the dissemination of online content related to terrorism or violent extremism in ~~crisis~~ situations, which stems from an ongoing or recent real-world event~~, depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population,~~ and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers."

As some MSs referred, there also lacks a description, what are Europol's competences in such situations. So we propose adding a clarification as a second section or creating a reference, if possible. As Commission said, this could refer informing the service providers by Europol. So the second section could set the criteria:

"In order to prevent dissemination of online content related to terrorism or violent extremism, Europol…" – and the competences are discussed among MS and the Commission and **actual capabilities that Europol possesses** + which are referred to in Crisis Protocol.

We would like to stress, that this is just a food for thought and in our view Europol's mandate would remain the same – Europol would take action if crisis protocol is triggered. Also we are not against, but rise this question since MSs expressed their concerns.

3) **"Transmission", "transfer" and also "forward"**. GDPR has not defined either of the terms, however in practice, as Commission explained, it is differentiated. If there is a clear distinction, this should to be clarified. If reading the proposal, "forward" is used only towards Europol => Member State. For example art. 26 para 6(e) uses only transfer and in English this causes confusion. Estonia proposes the following solution:

[1] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf

a) Set the terms under article 2 with clear distinctions which allows to use the terms logically throughout the regulation.

4) **Article 26(2)** – we see a new term of "establishing jurisdiction" and would like to confirm the meaning of the term. Europol may use private party data to identify the national units. If identified, it may forward the results immediately to the national units concerned in order to "establish the jurisdiction" – **in other words to establish in which MS the investigative initiative should be started?**

5) **Article 26(5) and article 26a(3)** – Estonia agrees with Belgium, that previous wording and logic was better and more restricting. In either way, criteria has to be fulfilled. Comment was made on article 26 para 5, but the latter article has exactly the same point and structure.

"5. Europol may **not** transmit or transfer personal data to private parties ~~on a case-by-case basis,~~ **except** where, **on a case-by-case basis**, it is strictly necessary, and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, in the following cases:"

6) **Article 26(6)(e)** – we agree with Germany, that if there are already references that limit the scope of transfers, specific reference under this paragraph "shall not be systematic, massive or structural", is not necessary.

7) **Article 26a** – only if article 4(1)(u) is changed, this article should be adjusted.

Research & innovation

1) **Article 4(4a)** – we just want to stress here the importance of the Swedish reasoning and conclude, that in our opinion this paragraph needs further discussion.

2) **Article 4(4b)** – the screening of foreign direct investments is indeed part of European Union strategic autonomy and the aim of this paragraph is noble and necessary. However, such regulations are not in place in all MS's, also currently not in Estonia (currently being drafted and discussed). Our question is: How Europol would conduct the support of these screenings?

3) **Article 33a(1)(g)** – concern is shared regarding the 1 year retention limit of logs. However, Europol should be granted an opinion here, whether they see risks and if, then which ones. However, we would like to discuss the additional sentence as an alternative.

"(g) the logs of the processing of personal data in the context of the project shall be kept for the duration of the project and 1 year after the project is concluded, solely for the purpose of and only as long as necessary for verifying the accuracy of the outcome of the data processing. **Europol, on a case by case basis, may request the extension of the logs up to 1 year within one month prior to ending of the period from the European Data Protection Supervisor**".

This would allow, on exceptional cases we currently can't predict, an option to prolong the retention of logs. Each time EDPS assesses the request and reasoning. Therefore, we find it unnecessary to add the criteria, which such cases may be – a project delay, after-analysis delay, a mistake has occurred etc.