CZECH REPUBLIC

On the involvement of Europol during the negotiations:

CZ **agrees to** (and prefers) the participation of Europol, which should be allowed to present its positions if requested, mainly as regards technical issues.

Drafting comments on document wk 757/2020 (CZ proposals marked in **red**):

Block 1

Article 4(1)(m)

The distribution of responsibilities in draft TCO regulation should be respected, as the Europol has no power to take down terrorist content online:

"(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including **in taking down of terrorist content online, and**, in cooperation with Member States, **the coordination of law enforcement authorities' response to cyberattacks~~, the taking down of terrorist content online,~~ and** the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;

Article 4(1)(u)

While we understand that the EU reaction to online content is still developing, we do not consider it wise to legislate on insufficiently defined area. We note that there has not yet been an evaluation of the activation of crisis protocol in November 2020. In addition, we note that recital 35, while helpfully illustrating expected support of Europol, does not really elaborate on the relevant instances. In particular, we suggest that definitions in the crisis protocol[1] be kept. In particular, relation to "**events of suspected criminal nature**" should be included.

Article 26(5

Even if we rely on the estimate of the Commission that all relevant situations are covered, at least the wording should be streamlined by deleting the word "**either**".

Article 26(3)

While this provision has not been changed, it scope is expanded considerably by expanding Art. 4(1)(m). Therefore, specification of application to referrals only appears necessary to prevent collision with other mechanisms, such as draft TCO regulation:

3. Following the transfer of personal data in accordance with point (c) of paragraph 5 of this Article, Europol may in connection therewith receive personal data directly from a private party which that private party declares it is legally allowed to transmit in accordance with the applicable law, in order to process such data for the **making of referrals of internet content** ~~performance of the task~~ set out in point (m) of Article 4(1).

Article 26(5)(c)

Similar to Art. 26(3), this provision should focus on referrals:

1 A crisis within the meaning of this Protocol constitutes a critical incident online where:
(1) the dissemination of content is linked to or suspected as being carried out in the context of terrorism or violent extremism, stemming from an on-going or recent real-world event which depicts harm to life or physical integrity, or calling for imminent harm to life or physical integrity and where the content aims at or has the effect of seriously intimidating a population; and
(2) where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.
A strong indicator of terrorist or violent extremist context is where the content is produced by or its dissemination is attributable to listed terrorist organisations or other listed violent extremist groups. The Protocol pertains only to online content stemming from events of a suspected criminal nature.

5. Europol may ~~not~~ **transmit or** transfer personal data to private parties ~~except where~~, on a case-by-case basis, where **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:**

…

(c) the **transmission or** transfer of personal data which are publicly available is strictly necessary for the **making of referrals of internet content** ~~performance of the task~~ set out in point (m) of Article 4(1) and the following conditions are met:

…

Article 26(6a)

In the light of the 2019 Council Conclusions, the replies to requests should be voluntary both for Member State's authorities and private parties (because the private party can find legal basis under GDPR or national rules). It should be also clear what the second subparagraph requires (legal basis for processing on the part of competent authority is not the same as duty of private party to reply established in domestic law). We believe that obligatory cooperation of private parties should be left to consideration of domestic legislator. Therefore we suggest following changes:

6a. The Member States may reply to requests by Europol ~~may request Member States~~, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.

Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. The cooperation of private parties is voluntary, unless otherwise provided for by Member State law.

Article 26a

CZ maintains its scrutiny reservation.

Article 26a(5)

In the light of the 2019 Council Conclusions, the replies to requests should be voluntary both for Member State's authorities and private parties (because the private party can find legal basis under GDPR or national rules). It should be also clear what the second subparagraph requires (legal basis for processing on the part of competent authority is not the same as duty of private party to reply established in domestic law). We believe that obligatory cooperation of private parties should be left to consideration of domestic legislator. Therefore we suggest following changes:

5. The Member States may reply to requests by Europol ~~may request Member States~~, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned. Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. The cooperation of private parties is voluntary, unless otherwise provided for by Member State law.

Block 3

Article 4(4a)

Neither this Article nor recital 11 suggest a solution for ensuring sufficient funding for research and innovation by Europol. Therefore, it is uncertain that the effects of new obligation to assist the Commission will have positive results.

Article 18(2)(e)

We understand that the Commission believes that all uses of operational data have been covered, but in light of data protection challenges we wish this provision to be future-proof. Therefore we suggest opening this purpose to all research activities covered by the Europol Regulation:

(e) research and innovation regarding matters covered by this Regulation, in particular for the development, training, testing and validation of algorithms for the development of tools;

Article 33a(1)

We believe that in (c), collaboration with Member States personnel should be promoted, subject to security protections:

(c) any personal data to be processed in the context of the project shall be temporarily copied to a separate, isolated and protected data processing environment within Europol for the sole purpose of carrying out that project and only specifically authorised staff of Europol and, subject to technical security measures, specifically authorised staff of Member States' competent authorities, shall have access to that data;

As regards (g), we believe that logs should be usable also for data protection enforcement and should be kept for 3 years, given that the tools are presumed to be deployed for a long term and specific concerns may arise in time:

(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~~ 2 (3) years 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 and auditing compliance with data protection rules.

(end of file)