CZECH REPUBLIC

Drafting comments on document wk 757/1/2020 REV 1:

Block 1

Article 2(r)

We welcome this definition; in order to align it fully with the Crisis Protocol[1], following changes are introduced:

"(r) "online crisis situation" means the dissemination of online content that is linked to or suspected as being carried out in the context of terrorism or violent extremism stemming from and ongoing or recent real-world event **of suspected criminal nature**, which depicts harm to life ...."

Article 4(1)(m)

In order to specify the coordination powers and reflect the distribution of responsibilities in draft TCO regulation, as the Europol has no power to take down terrorist content online, following redrafting is proposed:

"(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, **and, on request of a Member State, the coordination of law enforcement authorities' response to cyberattacks;"**

"referral of Internet content" should be defined in Article 2 to mean "referral 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";

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.

Article 26(2)

Obligation to identify "all" national units concerned could in theory lead to infinite or very long processing of received personal data. Therefore we suggest to add maximum limit for processing in the first sentence:

2. Europol may receive personal data directly from private parties and process those personal data**, for a period no longer than 6 months,** in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. ...

In addition, it would be strongly preferable for policy reasons to include in the second sentence the Member State of main establishment of private party among the national units notified:

Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned**, including the national unit of the Member State of the main establishment of such private party**.

Article 26(6a)

We support amended recital 31 and understand that there is only so much that may be provided for at EU level. Still, more can be done, while respecting the role of national legislators. 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). Therefore we suggest following changes:

6a. At the request of Europol, ~~may request~~ Member States, via their national units, may ~~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(5)

We support amended recital 31 and understand that there is only so much that may be provided for at EU level. Still, more can be done, while respecting the role of national legislators. 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). Therefore we suggest following changes:

5. At the requests of Europol Member States, via their national units, may ~~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

CZ supports changes already made in Articles 18(2)(e), 18(5), 33a(1)(c)(g) by the Presidency.

Article 4(4a)

CZ believes that the wording should focus more on:

(a) the research and innovation being done at Europol,

(b) the innovation monitoring and

(c) the support Europol gives to research prioritization by the Member States.

Certain parts of Art. 66(1)(2) of Frontex Regulation could be used in this regard.

Block 5

Article 25(5)

We propose to use the term "or category of transfers" to align the text with Art. 38(1) LED.

We also support to strengthen substantially the transfer tools available, similarly to those used by Eurojust. Situation of Schengen-associated countries should be clarified. As German delegation announced drafting proposal, CZ refrains from proposing particular wording at this moment.

Block 7

Article 6(1)

We refuse the proposed addition of "Member State or". While this proposal falls into scope of mandate of Europol under Art. 3(1), it is unnecessary, superfluous, burdensome and disproportionate. Already under existing rules, the Europol can and should send any information that may lead to start of investigations to relevant Member State. However, the formal mechanism

of Art. 6 is inappropriate for crimes that affect only that Member State and contravenes the principle of subsidiarity.

(end of file)