

EXECUTIVE SUMMARY

Pursuant to Article 18 of the Digital Service Act ('DSA'), and Article 14(5) of the Terrorist Content Online ('TCO') Regulation, Host Service Providers ('HSPs') are required, in presence of specific circumstances, to **transmit to Europol information (including personal data of the users of the online services) related to imminent threat to life or safety** ('TTLS') situations.

DSA and TCO notifications related to TTLS situations have become part of a regular flow of work for the Operations Department at Europol. Currently, Europol relies on an 'internal manual process' to process personal data received from HSPs through TTLS notifications.

This Supervisory Opinion is issued in reply to a Europol's prior consultation concerning a new processing operation designed to enable the - partially automated - intake and handling of TTLS notifications received from HSPs. Europol envisages the implementation of a new workflow in PERCI to process ('open source' or 'closed') personal data transmitted or transferred by HSPs. This processing operation is part of a set of new functionalities incorporated into the PERCI (*Plateforme Européenne de Retraits des Contenus Illégaux sur Internet*) solution.

The EDPS found that the new workflow in PERCI materially alters the nature and scale of the processing that currently applies to data transmitted or transferred to Europol by private parties pursuant to Article 18 DSA and Article 14(5) TCO. Such substantial modifications raise new risks for data subjects. These risks are linked to the various forms of processing that Europol envisages to perform when handling personal data included in TTLS notifications submitted by HSPs via the new PERCI workflow.

The 2022 amendment of the ER entrusted Europol **enhanced powers to process personal data received from private parties**. The increasing reliance on data originating from private parties to carry out Europol's tasks raises specific data protection challenges. Such **challenges are inherent to the use, by law enforcement authorities, of personal data originally collected and processed for economic purposes**.

Under the current legal framework, specific safeguards apply to the various types of processing operations that Europol is entitled to carry out in relation to personal data received from private parties, including TTLS-related information transmitted by HSPs pursuant to Article 18 DSA, or 14(5) TCO. Such safeguards uphold key principles - including lawfulness, necessity, proportionality, purpose limitation, data accuracy, data retention - underpinning data protection rights, as well as data security, transparency, and accountability obligations.

Based on the documentation provided by Europol, the EDPS found that some of the processing operations to be performed under the new PERCI workflow would not be consistent with the rules and limitations that the ER sets out to implement cooperation with private parties.

Europol indicates that, pursuant to the requirement set out under Article 26(2) of the Europol Regulation ('ER'), personal data included in TTLS notification shared by HSPs will **be processed within the PERCI environment for the sole purpose of identifying**

the concerned Member State(s). Upon identification of the concerned Member State(s), Europol will forward, unaltered, the HSP notification to the relevant competent authorities.

At the same time, **Europol will have the possibility to process personal data included in HSPs' TTLS notifications outside of the PERCI environment.** The EDPS notes that Europol did not clarify the purposes and conditions applying to the processing, within Europol's operational environment, of personal data received from HSPs via PERCI. Ensuring clarity in this regard is of utmost importance to ensure compliance with the legal framework that regulates exchanges of personal data between private parties and Europol.

In order to ensure compliance with Article 26(2) ER, the **EDPS deems necessary** for Europol to specify that any processing operation performed outside PERCI in relation to personal data received through TTLS notifications transmitted by HSPs is only to be carried out for the specific purpose of identifying the competent authorities concerned, and responsible to address the imminent threat to life or safety of persons Europol should also ensure that personal data received via the PERCI workflow on the basis of HSPs' TTLS notifications is only processed to the extent (scope and time) that is necessary and proportionate to address the imminent threat to life and safety of persons concerned.

Before data received through HSPs notifications via PERCI is ingested into Europol's operational environment, Europol should carry out specific checks, including:

- a *lex specialis* check to verify the applicability of Articles 26a, or 26b ER;
- a mandate check to confirm that the data received fall within Europol's mandate and ensure that the processing of such data is necessary and proportionate to the performance of the agency's tasks.
- a data subject categorisation ('DSC') process to establish whether the categories of data subjects listed in Annex II of the Regulation are identified, on the basis of the information provided by the private party.

The EDPS further notes that clear storage limitation(s) have not been defined with regard to personal data imported in PERCI and processed within that environment. Europol did neither specify which data retention period would apply to personal data received by Europol on the basis of TTLS notifications transmitted by HSPs via PERCI, and consequently transferred to Europol's operational environment.

In order to ensure compliance with Article 26(2) ER, the **EDPS deems necessary** that Europol clearly indicate the period(s) of time after which personal data transmitted to Europol via PERCI will be erased from PERCI, and from Europol's operational environment. Data retention period(s) applying to the personal data received from HSPs via PERCI should be commensurate to the underlying processing purpose (i.e. to identify the Member State(s) concerned by the TTLS) as well as to the operational objective underpinning the envisaged processing operation (i.e. support Member States in addressing situations of imminent threat to life and safety of persons).



