EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr [...]
Data Protection Officer Europol
Eisenhowerlaan 73
NL-2517 KK The Hague
The Netherlands

Brussels, 7 September 2018
WW/BR/sn/D(2018)1990 **C 2018-0628**

Subject: Europol's consultation on law enforcement access to WHOIS database

Dear Mr [...],

We refer to your consultation of 5 July 2018 concerning European law enforcement authorities' ('LEA') access to personal data contained in the WHOIS database. We thank you for your comprehensive summary, analysis and the supporting documents.

In your letter you explain that the entry into force of the EU's General Data Protection Regulation (GDPR) has impacted LEAs' access to the publicly available and decentralized WHOIS database of registration and contact information of registrars and registrants of domain names. You explain that since the entry into force of GDPR, ICANN has issued a specification mandating registries and registrars to redact all personal data from publicly available WHOIS records. This led to the loss of LEAs direct access to personal data of registrants of domain names. ICANN requires LEAs, which would like to access the WHOIS datasets, to conclude formal legal procedures to obtain relevant information. This leads to substantial administrative burdens and long delays for LEAs. This obstacle tor LEAs to access WHOIS records led to a debate between ICANN and the Article 29 Working Party (now the European Data Protection Board) on how to improve LEAs' access to the WHOIS database. Europol's consultation refers to three scenarios regarding a possible role of Europol in this context.

Please find hereunder the EDPS' analysis in respect to the three scenarios.

- Scenario 1

Europol would act as a "simple LEA accreditor", giving assurances to the registries and registrars that individual EU-based LEAs approaching them for access to non-public WHOIS are a legitimate law enforcement agency. Europol mentions in this respect that although this scenario does not involve the processing of personal data by Europol, it would still have a data

protection implication in the sense that the "accreditation authority" would probably be scrutinised against Article 41 GDPR.

The EDPS believes that Europol could act as a "law enforcement accreditor" under this scenario, as long as this activity falls within its mandate.. In this respect, Article 4(1)h of the Europol Regulation ('*Support members States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing operational, technical and financial support*') seems to be relevant. However, as pointed out by Europol, this scenario would not involve the processing of personal data by Europol. Therefore, it does not raise matters within the competence of the EDPS' supervision tasks. Furthermore, since Europol's accreditor role would not lead to the processing of personal data, Article 41 GDPR would not apply. In any event, in the EDPS' view Europol's role would not fall under Article 41 GDPR. Indeed, Europol would not monitor compliance with a code of conduct, but would merely certify that a LEA approaching registrars and registries is a legitimate LEA.

With regard to Scenarios 2 and 3 mentioned in your consultation, the EDPS believes that they cannot be based on the Europol Regulation.

- Scenario 2

Under this scenario, Europol would provide a common European web-platform for accredited EU LEAs to query non-public WHOIS databases. This option would exempt individual EU Member States of having to build their own web-platform. Europol would only act as a facilitator and provide the necessary technical infrastructure for the EU member states to query the databases. Europol would not have access to the information exchanged between the EU Member States and the private companies.

The EDPS does not see a legal basis for Europol's provision of such web-platform, which would facilitate the exchange of information, including personal data. Such a provision of a web-platform cannot be based on Articles 18(2)(d) and 38(7) of the Europol Regulation. This provision enables Europol to facilitate bilateral data exchanges between actors mentioned in this Article. However, ICANN is a private party under the form of a corporation and does not qualify as an international organisation as required by the above-mentioned provisions.

- Scenario 3

Under this scenario, Europol would act as information exchange facilitator. Europol would also have direct access to exchanged information and the possibility to add operational value.

The EDPS does not see a legal basis for this scenario. On the one hand, this scenario raises an issue with Article 26(9) of the Europol Regulation, stipulating that Europol may not contact private parties to retrieve personal data. On the other hand, such an access does not seem to fall under Europol's objectives as laid down in Article 3 of the Europol Regulation nor under any processing purpose of Article 18 of the Europol Regulation. Therefore, Scenario 3 is not covered by the current Europol Regulation.

We remain at your disposal for any further information.

Sincerely yours,

(signed)

Wojciech Rafał WIEWIÓROWSKI