EDPS OPINION ON A PRIOR CONSULTATION REQUESTED BY EUROPOL

on the European Platform for takedown of illegal content online (Plateforme Européenne de Retraits des Contenus illégaux sur Internet - 'PERCI')

(Case 2022-0284)

1. PROCEEDINGS

On **2 March 2022**, the EDPS received a request for prior consultation from Europol under Article 39 of Regulation (EU) 2016/794 ('Europol Regulation)[1] on PERCI.

The prior consultation request contained the following:

- The formal notification of the prior consultation, with an identification of four risks and a filled-out questionnaire by Europol's staff [2];
- A cover letter from Europol's DPO to the EDPS [3];
- A document providing an explanation of CLOUD II and an inventory of copies of the Contracts under CLOUD II (European Commission - DG DIGIT);
- A Microsoft's document of December 2019 about Microsoft Azure entitled 'Azure Data Residency and Protection';
- A document concerning Azure data encryption (European Commission Cloud II – DPS 1 Mini-competition MC2, Microsoft)
- A document providing an explanation on how to know if an azure service is available in EU regions (European Commission - DG DIGIT);
- A document providing information on access to customer data - Azure Customer Lockbox (European Commission Cloud II – DPS 1 Mini-competition MC2, Microsoft);
- A document compiling information related to the protection of personal data in the CLOUD II procurement procedure (European Commission - DG DIGIT);

---

1 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114.

2 EDOC#1214010.

3 EDOC#1214009.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

- A document titled: Governance, Security and Compliance (European Commission - DG DIGIT);
- The hybrid Cloud Initiative 2020 - Approach [4];
- The PERCI Workflow state diagram [5];
- The Dynamic Purchasing System For Cloud Services (Reference DIGIT/A3/PR/2018/035 CLOUD II DPS 1 MC2) Direct Contract 2020-9906 (with Microsoft Ireland Operations Limited) [6];
- The PERCI Access Matrix[7] ;
- The PERCI Security & Compliance Considerations [8];
- The Dynamic Purchasing System For Cloud Services (DIGIT/A3/PR/2018/035 CLOUD II DPS 1 MC1) Direct Contract 2020-1742 (with Amazon Web Services) [9];
- The prior consultation form with regard to Member States' MS remote access to the Internet Referral Management application (IRMa) [10];
- The EDPS Opinion on the prior consultation regarding the 'Internet Referral Management Application' (IRMa), EDPS Case 2017-0954 [11];
- CLOUD II DPS 1 MC2-w ithoutFinancial.PDF EDOC[12].

On **28 March 2022**, the EDPS sent a request for additional documentation/information to Europol requesting the agency to submit their replies by 19 April 2022. In particular, the EDPS requested additional documentation such as the detailed security plan for PERCI, the procedure of the access control mechanism of the Europol Platform for Experts System ('EPE'), a tentative description of the audit control requirements that will be provided by the Azure Cloud and a specific time plan on implementing the audit logs in the Unified Audit Solution, the current Europol's Cloud Strategy and two documents that were referenced by Europol but not submitted[13]. The EDPS also requested information as to whether the current IRMa system and its data will be migrated to the new PERCI system, on the management of the decryption keys, on the Transfer Impact Assessment that Europol should have carried out in order to ensure compliance with the applicable data protection legal framework and on the reasoning for opting for the Cloud II framework contract for procuring services with regard to operational data (the processing of which is regulated by the Europol Regulation).

On **1 April 2022**, during a bi-monthly meeting held between Europol and the EDPS at staff level, the EDPS reminded Europol of the investigation launched regarding the use of cloud services provided by Microsoft under Cloud II contracts by European Union institutions, bodies and agencies (EUIs) and the extent to which Europol is impacted by this investigation.

---

4 EDOC#1097840-v4.
5 EDOC#1168868-v11.
6 EDOC#1180310-v1.
7 EDOC#1185675-v1.
8 EDOC#1214344-v1.
9 EDOC#1217523-v1.
10 EDOC # 910139-v.3.
11 EDOC-#949325-v1.
12 EDOC#1145817v3.
13 EDOC #1165154 and EDOC#919844.

The EDPS highlighted during this meeting that the risks for the data subjects identified in the context of the specific investigation can only be magnified in the context of processing operational data[14].

On **19 April 2022**, Europol requested an extension of the deadline for the submission of their reply.

On **5 May 2022**, Europol submitted another request for extension of the deadline. The EDPS informed Europol that, given the strict legal deadline for the EDPS to issue its opinion under Article 39 ER, it would not accept any additional documentation after the 29 May 2022.

Europol submitted their replies on **25 May 2022.** With their reply[15] Europol provided new documentation and **amended the prior consultation notification**[16] initially submitted to the EDPS with regard to the development and testing approach for the delivery of PERCI. The modification refers to the use of personal data collected from publicly available sources during the development of the software for PERCI and to the use of operational production data (removal orders) for the effective testing of the PERCI solution. Europol also informed the EDPS that on 10 May 2022 they had decided to stop the development and testing of the affected parts of PERCI waiting for further guidance from the EDPS. In particular, Europol's reply included the following additional documentation:

- Draft hybrid cloud strategy[17] and related Security Policy[18];
- User management policy of the EPE[19];
- Data protection requirements baseline[20];
- EUROPOL draft specific (sub)processor analysis[21];
- Draft PERCI security design[22];
- EUROPOL's security service level agreement with DIGIT - Appendix A.5 related to cloud brokerage[23];
- Direct Contract 2020-9906 Cloud II DPS1 MC[24];
- Description of PERCI data fields[25];

On **3, 9 and 15 June 2022**, the EDPS and Europol held staff level meetings to clarify issues concerning the use of personal data for the development and testing of the PERCI application, the management of the decryption keys and possible Microsoft access to

---

14 Relevant press release.
15 EDOC##1224686v20.
16 EDOC#1231556v7.
17 EDOC #1139219v4D.
18 EDOC #708779v6.
19 EDOC #734013v12.
20 EDOC #919844v10.
21 EDOC #1228993v2.
22 EDOC #1210967v2B.
23 EDOC #1031427v24.
24 EDOC #1112397v4.
25 EDOC #1226990v1.

Europol's data as well as the reasoning for opting for the Cloud II framework contract for procuring services with regard to operational data.

On **8 June 2022**, Europol provided a further set of replies[26].

According to Article 39(3) of the Europol Regulation, the EDPS is to issue his Opinion to the Europol Management Board within a period of two months following the receipt of the notification of the prior consultation. That period may be suspended until the EDPS has obtained any further information requested and for a maximum period of two additional months, after which the opinion shall be deemed favourable.

In this case, the deadline for the EDPS' response was suspended for 58 days, meaning the deadline within which the EDPS shall issue his Opinion is **27 June 2022**.

2. DESCRIPTION OF THE PROCESSING

2.1. Background and brief description of the main characteristics and main changes introduced by PERCI

PERCI, which is the successor of IRMa (Internet Referral Management application), will provide Member States and Europol with a technical solution for managing referrals and removal orders to hosting service providers ('HSPs') for the removal of terrorist content online.

This was considered necessary in order to meet the new obligations and requirements established in Regulation (EU) 2021/784[27] on addressing the dissemination of terrorist content online, which became applicable on 7 June 2022. One of the new rules established in Regulation (EU) 2021/784 is that alongside referrals, Member States' competent authorities shall have the power to issue removal orders requiring hosting service providers to remove or disable access to terrorist content in all Member States.

The Regulation (EU) 2021/784 encourages Member States to make use of dedicated technical solutions (tools) developed by Europol '*such as the current IRMA or its successors*' to support the implementation of its provisions at national level.[28] The dedicated tools established by Europol may in particular facilitate the processing and feedback relating to removal orders for Member States and hosting service providers.[29]

---

[26] Without EDOC number.

[27] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), OJ, L 172, 17.05.2021, p. 79-109.

[28] Recital 39 of Regulation (EU) 2021/784.

[29] Article 14(4)(a) and (b) of Regulation (EU) 2021/784.

As currently established, IRMa is Europol's dedicated tool for the notice and take down procedure, i.e. the sending of referrals to hosting service providers for the removal of terrorist content online pursuant to Article 4(1)(m) of Europol's Regulation. IRMa is accessible by authorised staff of Europol's EU Internet Referral Unit (EU IRU), as well as a limited number of authorised users from competent authorities in Belgium, France, Germany, Italy, Netherlands, Portugal and Slovenia. IRMa was established for the management of referrals and does not support the processing of referrals and removal orders by all Member States at scale.

Building upon the functionalities and workflow of IRMa, Europol considers that PERCI will provide Member States and Europol with the advanced technical solution needed to meet the new obligations and requirements established in Regulation (EU) 2021/784. In addition to Europol users, PERCI will be accessible by users in Member States' competent authorities on a 24/7 basis. Access to it will be provided via secure Internet connection to these designated competent authorities.

One of the substantial changes to IRMa is the move to the Cloud. Technically, while IRMa is a system hosted within Europol infrastructure (on-premise), which has been prior consulted with the EDPS[30], PERCI will be hosted on the Microsoft Azure Cloud.

In more detail, PERCI data (including URLs, downloads of the publicly available content - including sensitive data as racial or ethnic origin, religious, philosophical beliefs, etc - screenshots as visualised by a web browser, other online identifiers such as email addresses, social media account handles, usernames, and IDs that are publicly available) is persisted[31] in the Azure Cloud platform using block storage, object storage and relational databases. In addition, Azure cloud administrators' data, i.e. account identifiers of Europol personnel managing Europol's Azure administrative accounts are included in the data processed in the platform. The storage infrastructure is offered as a managed service by the Microsoft Azure Cloud provider.

Responsibility and actual management of the stored data lies with Europol. The EDPS understands[32] that Europol is planning to encrypt their data using Microsoft's built-in encryption solution using 256-bit AES encryption. This encryption cannot be disabled[33].

Key management in the Europol Azure Tenant will be done by leveraging the Azure KeyVault Premium with HSM (Hardware Security Module) service and customer managed keys capability. It is planned that Europol will deploy customer managed keys for all data-at-rest encryption in the Cloud environment before the go-live of the platform. Europol assessed the

---

30 Case 2017-0954.

31 Persisted is a computer science term that in this context means: ensure data existence in the cloud by being present in 'different technical ways' which also prevents the data to be deleted by mistake. This also ensures the usability of the data in different modes/ways.

32 EDOC#1214010, section 'Storage of content'.

33 EDOC#1214010, p. 22 under Q8.

BYOK (Bring-Your-Own-Key) approach but discarded it as it was considered not feasible to be applied within the project timeframe, i.e. to meet the deadline of 7 June 2022. Currently Europol does not have an Azure compatible HSM to generate its own keys. The key usage on the system is designed to allow a future migration to Europol generated keys once a suitable HSM is available to generate them.[34]

PERCI will not be used for purposes of operational analysis, for cross-checking or for analysis of a strategic or thematic nature. PERCI will not interact with other Europol databases and information systems. At their discretion, Member States' competent authorities will have the possibility to request the provision of operational support by Europol on the basis of content they have processed in PERCI. Such requests will follow the ordinary procedure applicable to the sending of contributions to Europol, i.e. Member States' competent authorities will have to send a message to Europol via SIENA with the relevant purpose indication towards an operational analysis project[35].

2.2. Detailed description of PERCI data flow

[redacted]

[34] EDOC#1224686v20, p. 8 under 2.4.
[35] EDOC#1214010, p. 16 under Q2.

[redacted]

[redacted]

2.3. Software development and testing [38]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[38] EDOC # 1231556 v 7.

[redacted]

3. Legal and technical assessment

3.1. Need for prior consultation pursuant to Article 39 of the Europol Regulation

Article 39 of the Europol Regulation subjects some processing operations to prior consultation by the EDPS. According to Article 39(1) of the Europol Regulation, the scope of application of the prior consultation requirement covers:

(a) processing of special categories of personal data as referred to in Article 30(2); or
(b) types of processing, in particular using new technologies, mechanisms or procedures, presenting specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.

Furthermore, according to Recital 50 of the Europol Regulation: '*the prior consultation mechanism is an important safeguard for new types of processing operations. This should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new IT systems for the processing of personal data* ***and any substantial changes thereto***'.

In the case under consideration, the processing operations described by Europol include the processing of special categories of personal data (Article 30(2) ER) and in particular of data relating to racial and/or ethnic origin, political opinions, religious and/or philosophical beliefs[42].

[39] EDOC#1231556v7 (amendment to the prior consultation notification).

[redacted]

[42] EDOC#1214010, p. 17-18 under Q6 and Q6-1.

Furthermore, they represent a '*substantial change to the manner of processing*' personal data by using new technologies and in particular by using for the first time cloud computing services.

The use of cloud computing services presents specific risks for the data subjects that need to be carefully addressed (e.g. confidentiality risks, risks stemming from the failure to identify the appropriate data protection legal framework, risks stemming from transfers of operational data to third countries without an adequate level of protection, lack of appropriate auditability etc), which have to be clearly identified and mitigated through the Article 39 ER procedure.

In view of the above, the EDPS confirms Europol's assessment that the development and operation of PERCI **is subject to prior consultation** in accordance with Article 39(1)(a) and (b) of the Europol Regulation.

3.2. Scope of the Opinion

The Opinion of the EDPS on this prior consultation concerns the processing operations necessary for the development and operation of PERCI for the management of referrals and removal orders to hosting service providers for the removal of terrorist content. While the request for prior consultation was submitted under Regulation (EU) 2016/794 of 11 May 2016 (the 'Europol Regulation'), and taking into account the proximity of the issuance of this Opinion and the entry into force of the amended Europol Regulation[43], we base our analysis on the latter as well.

3.3. Europol's legal basis for the development and operation of PERCI

As reported in the notification, the processing operations in the context of PERCI relate to the task laid down in Article 4(1)(m) ER[44]: '*support Member States' actions in preventing and*

[43] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, PE/8/2022/REV/1, OJ L 169, 27.6.2022, p. 1–42 will enter into force on 28 June 2022.

[44] Article 4(1)(m) is amended as follows by Regulation 2022/991: ' *(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 by:*
(i) assisting the competent authorities of the Member States, upon their request, in responding to cyberattacks of suspected criminal origin;
(ii) cooperating with competent authorities of the Member States with regard to removal orders, in accordance with Article 14 of Regulation (EU) 2021/784; and
(iii) making referrals of online content to the online service providers concerned for their voluntary consideration of the compatibility of that content with their own terms and conditions'.

combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the hosting service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions'.

In addition, Regulation (EU) 2021/784 provides that alongside referrals, Member States' competent authorities shall have the power to issue removal orders requiring hosting service providers to remove or disable access to terrorist content in all Member States (Article 3). This Regulation further encourages Member States to make use of dedicated technical solutions (tools) developed by Europol '*such as the current internet Referral Management application or its successors*' in order to support the implementation of its provisions at national level and in particular to facilitate the swift exchanges between competent authorities and hosting service providers (relating in particular to removal orders), to avoid duplication of effort, to standardise the exchange of information, to reduce costs for the implementation of the notice and take down procedure, and to contribute to a higher standard of the process (Article 14(4)(a) and (b), recital 39, recital 46).

The EDPS considers that even if support for the removal orders, the main new functionality provided by PERCI, is not expressly mentioned in Article 4(1)(m) ER, the indicative wording of this Article read in conjunction with Regulation (EU) 2021/784 provides sufficient legal basis for the processing of personal data in the context of a functioning PERCI and falls under the purpose of Article 18(2)(d) ER [45].

PERCI will facilitate the access to and the exchange of data between Member States, Europol and third parties (hosting service providers) as part of Europol's support to Member States' actions in preventing and combating serious crime and terrorism.

PERCI will also allow Europol (EU Internet Referral Unit) to perform referrals in the exercise of its task under Art. 4(1)(m) ER, and under its role described in Regulation (EU) 2021/784. Thus, we observe that Europol acts in this context both as provider of advanced IT solutions/services to Member States and as party to the exchange of information about referrals.

PERCI will serve exclusively the purpose of supporting Member States' competent authorities complying with their notice and take down obligations resulting from Regulation (EU) 2021/784 as it will be the tool dedicated to the making of referrals and the transmission of referrals and removal orders to the hosting service providers concerned in line with the abovementioned Regulation. The transmissions via PERCI will also allow to avoid duplication of work, easier de-confliction between parties concerned, as well as the standardisation of the notice and take down procedure. It thus adds to the efficiency of mutual cooperation between Member States and Europol.

---

[45] Article 18(2)(d) is amended as follows by Regulation 2022/991: '(d) *facilitating the exchange of information between Member States, Europol, other Union bodies, third countries, international organisations and private parties*'.

Given the above, the processing of information, including personal data, in the context of the operation of PERCI **falls within Europol's tasks provided in Article 4.** Furthermore carrying out referrals of Internet content falls **under the purpose of Article 18(2)(c)** while the provision of advanced IT solution/services to Member States falls **under the purpose of 18(2)(d)** of the Europol Regulation.

3.4. Assessment of the risks to data subjects from the development and operation of PERCI

3.4.1. Risks identified by Europol

Under Article 39(2) ER, four elements should be present in each prior consultation of the EDPS: (1) a description of the process or system that is being consulted, (2) an assessment of the specific risks posed by this process or system, (3) the mitigating measures that Europol plans to apply in order to mitigate these risks where possible, and (4) additional '*safeguards and mechanisms to ensure the protection of personal data*'.

The risk assessment table included in Europol's prior consultation form on PERCI includes four risks. The following three risks identified by Europol are related to the use of Cloud computing services:

1. Unauthorised Access;
2. Confidentiality and integrity risks for data;
3. Lack of audit integration in UAS.

The last one identified by Europol refers to the unauthorised secondary use of sensitive personal data.

The EDPS considers that the mitigation measures recommended are appropriate to limit the risks to an acceptable level.

3.4.2. Other potential areas of risk

The EDPS notes that Europol does not have identified specific areas of potential risk that arise from (i) Europol's decision to assign the processing of operational data to a processor (private party) and the failure to conclude appropriate contractual clauses; (ii) the possible transfers of Europol's data to private parties in third countries acting as processors stemming from the use of cloud computing services; (iii) the development and testing of PERCI application with personal data and (iv) the lack of an adopted Cloud Strategy.

3.4.2.1. Risks stemming from the failure to conclude appropriate contractual clauses that would ensure that the processor meets the requirements of the applicable legal framework

The operation of PERCI entails that the processing (concretely the storing) of operational data is contractually assigned to a private party, i.e. Microsoft Ireland which is acting as a processor. This raises the issue of defining the requirements that the processor should meet in order for the controller to comply with the legal framework in place.

The Europol Regulation, contrary to Chapter IX of Regulation (EU) 2018/1725 ('EUDPR')[46], does not include any provisions regarding the requirements that a processor should meet in case they are processing operational data on behalf of the controller.[47] This will however change with the entry into force of the amended Europol Regulation, which will subject Europol to Chapter IX of the EUDPR[48].

Article 87(1) EUDPR provides that the controller shall only use processors providing sufficient guarantees that the '*processing will meet the requirements of this Regulation and the legal act establishing the controller and ensure the protection of the rights of the data subject*'. In other words, as soon as the amended Europol Regulation will enter into force and Chapter IX EUDPR will also apply to the processing of operational personal data by Europol (Article 27a of the amended ER) a service offered by a processor to Europol with regard to operational data shall comply with the requirements provided in chapter IX EUDPR and in the respective provisions of the Europol Regulation.

Hence, the EDPS considers that the same approach should be followed under the current legal framework as the underlying reasoning remains the same (the nature of the processing in the law enforcement context justifies that the processor adheres to the same obligations as if the processing were carried out by the controller). Consequently, the contract concluded with a processor for the processing of operational personal data shall ensure that the processor meets the requirements of the Europol Regulation.

Contrary to the above, Direct contract No 2020-9906 (EDOC #1180310) provides, in between others, that the Contractor (i.e. Microsoft Ireland) shall meet the requirements provided in EUDPR (clause 12.2.4), shall assist the Controller to respond to requests for exercising the rights of person whose personal data is processed in relation to this Contract as laid down in Chapter III (articles 14-25) of EUDPR (clause 12.2.5), shall assist the Controller for the fulfilment of its obligations pursuant to articles 33 to 41 EUDPR (clause 12.2.11) and shall ensure that any potential transfers shall fully comply with Chapter V of EUDPR (clause

---

[46] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), OJ L 295, 21.11.2018, p. 39–98.

[47] Indeed, the ER does not seem to contain a general provision authorising Europol to make use of processors for the processing of operational data.

[48] Article 27a(1) inserted by Regulation 2022/991, OJ L 169, 27.6.2022, p. 1–42, provides that '*Without prejudice to this Regulation, Article 3 and Chapter IX of Regulation (EU) 2018/1725 shall apply to the processing of personal data by Europol*'.

12.2.3) and not with the specific provisions of Chapter IX EUDPR and of the Europol Regulation.

Europol is of the opinion that '*while the FWC in question starts from the premise of the processing of data in accordance the EUDPR, this does not limit the legal basis for data processing by the data controller in using the FWC. In Europol's case, the Europol Regulation (ER), as the corresponding legal basis, is connected to the processing purposes specified in Art. 18 of the ER. The data protection and security conditions are connected to those processing purposes. Concerning the suitability of the FWC and the envisaged cloud services, the measures in place for the protection of data by those services and the additional Europol specific safeguards were assessed by Europol as adequate, for the particular use in the operational context of PERCI, taking into account the nature of the processing, the volume, the users and the types of data. It is also evident that cloud services are required to deliver the PERCI solution*'.

Nevertheless, the EDPS notes that as analysed above the respective Cloud II framework contract does not provide the appropriate contractual framework for Europol's cooperation with Microsoft as it does not ensure that the processor will meet the requirements of the Europol Regulation with regard to (indicative listing) data subjects' rights, international transfers, security of the processing operations. These requirements cannot be dependent on the volume and types of operational data under processing. This issue will not be remedied by the entrance into force of the emended Europol Regulation.

In view of the above, **the EDPS considers that the respective Cloud II framework contract as is does not ensure that the processor will meet the requirements of the Europol Regulation and therefore creates a risk of non-compliance with the provisions of the Europol Regulation.**

This issue will not be remedied by the entrance into force of the amended Europol Regulation as the respective Cloud II framework contract **will not ensure that the processor will meet the requirements of Chapter IX EUDPR as specified by the amended Europol Regulation and therefore a risk of non-compliance will be created with the provision of Article 87 EUDPR and the amended Europol Regulation, in particular with regard to the provisions regulating data subjects' rights, accountability, international data transfers and the security of the processing operations.**

The EDPS thus recommends that Europol ensures that the contractual framework binds the processor to meet the requirements of the Europol Regulation and as of 28 June 2022 of Chapter IX EUDPR as specified by the amended Europol Regulation. This could take place either in or outside the context of the respective Cloud II framework contract.

3.4.2.2. Risks stemming from possible transfers to private parties in third countries acting as processors

Article 25 and 26 of the Europol Regulation, also under the amended Europol Regulation, as well as Article 94 EUDPR[49] that regulate transfers of operational data to third countries do not include in their scope transfers to private parties acting as processors.

Article 25 ER (as in force and as amended by Regulation 2022/991) and 94 EUDPR provide for transfers to competent authorities in third countries and to international organisations and for the respective 'transfer tools'. When the amended Europol Regulation will enter into force, these 'tools' will be the Commission's adequacy decisions, international agreements pursuant to Article 218 TFEU, cooperation agreements concluded before 1 May 2017 and appropriate safeguards provided either in a legally binding tool or stemming from the circumstances surrounding the transfer.

Article 26 (as in force and as amended by Regulation 2022/991), on the other hand, provides for specific cases where transfers are allowed to private parties. When the amended Europol Regulation will enter into force, such transfers will be allowed if undoubtedly in the interest of the data subject; absolutely necessary in the interests of preventing the imminent perpetration of a crime, including terrorism; personal data is publicly available and the transfer is strictly necessary for the performance of the task set out in point (m) of Article 4(1); the transfer is strictly necessary for Europol to inform that private party that the information received is insufficient to enable Europol to identify the national units. In case the private party is not established within the Union or in a country with regard to which a 'transfer tool' of the ones mentioned in Article 25 exists, then the requirements for transfers will be even more stringent (transfers shall only be authorised by the Executive Director when it is necessary in order to protect the vital interests of the data subject; to safeguard legitimate interests of the data subject; for the prevention of an immediate and serious threat to public security; for the purposes of the prevention, investigation, detection or prosecution of a specific criminal offences; and for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence). Thus, transfers of operational data to private parties in third countries acting as processors are not allowed neither by the Europol Regulation in force nor as of 28 June 2022 by Chapter IX EUDPR as specified by the amended Europol Regulation.

On 28 March 2022, the EDPS had asked Europol to provide him with the Transfer Impact Assessments carried out in order to ensure compliance with the applicable data protection legal framework in the context of transfers prima facie entailed by hosting PERCI on Microsoft Azure. Europol did not provide any Transfer Impact Assessment as according to

[49] As analysed under 3.4.2.1. given the proximity of the issuance of this Opinion and the entry into force of the recast of the Europol regulation, we base our analysis on the latter as well.

the Agency no transfers of personal data are taking place in the context of hosting PERCI in the cloud.

To this end and under the condition that the investigation with regard to the use of cloud services provided by Microsoft under Cloud II is still pending[50], the EDPS notes the following:

According to clause 11 of the Direct Contract[51], transfers of personal data (both customer data and non-customer data[52]) are allowed under the specific conditions provided in this clause.

Second, according to clauses 3.2.3 and 3.2.4 of Annex IV - Service Level Agreement (SLA) for Cloud services, there exist services for the provision of which data may leave the territory of the EEA [53]. We note that the Appendix I containing the list of such services, was not submitted

---

[50] Following the ruling in the Schrems II Judgement, the EDPS opened in May 2021 two investigations, one of which is the investigation with regard to the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts. Although, the Commission is the primary addressee of this investigation as the 'lead contracting authority' and 'cloud broker' for the EUIs' procurement of Microsoft cloud services under the respective Cloud II direct contract, the investigation extends to all other EUIs as controllers in so far as deemed necessary, hence to Europol as well. While, the EDPS is not in a position to draw any definitive conclusion on the compliance of these services with the data protection legal framework in place until the end of the EDPS' investigation, we can already identify in the present Opinion the areas of concern that should be carefully assessed by Europol.

[51] EDOC#1180310-v1.
In more detail, the Direct Contract provides that:
'11.2 The Contracting Authority shall be able to ensure that its data remains at rest and in transit in the territory of the European Economic Area. The Contracting Authority may provide exceptions where the Contractor can document that adequate measures to protect the confidentiality of the data (e.g. encryption, etc.) are implemented. The Contractor must document the protective measures in writing. Such exceptions must be documented in the Contracting Authority's SLA and their usage agreed upon between the parties.
11.3 Services not in relation with the Contracting Authority's data (e.g. maintenance of the platforms, support) can be performed outside the European Economic Area. The list of these services must be documented in the Contracting Authority's SLA'.

[52] EDOC#1180310-v1, Direct Contract 2020-9906, Annex III - Contractors tender, 'Azure Data Residency and Protection' provides on page 5 definitions for the following data categories as established by Microsoft:
'*• **Customer data** is all data that customers provide to Microsoft to manage on customer's behalf through customer's use of Microsoft online services.*
*• **Customer content** is a subset of customer data and includes, for example, the content stored in a customer's Azure Storage account.*
*• **Personal data** means any information associated with a specific natural person, e.g., names and contact information of customer's end users. However, personal data could also include data that is not customer data, such as user ID that Azure can generate and assign to each user – such personal data is considered pseudonymous because it cannot identify an individual on its own.*
*• **Support and consulting data** mean all data provided by customer to Microsoft to obtain Support or Professional Services*'.

[53] The relevant clauses provide that:
'3.2.3. Services for the provision of which data may leave the territory of the European Economic Area
Pursuant to Article 11.2 of the Direct Contract, the list of services for which Customer data cannot entirely reside in the European Economic Area is:
- *CDN services (Content Delivery Networks)*

by Europol to the EDPS and is only '*submitted with the Contractor's tender and stored by the Commission*'. Moreover, the 'Azure Data Residency and Protection' document provided by Europol with the prior consultation notification contains different exceptions to data residency, e.g. for different Azure non-regional as well as regional services[54], to provide customer support and troubleshooting[55], or to respond to government requests for customer data[56].

Third, Annex IX – List of subprocessors lists 63 sub-processors (whether Microsoft entities or others) in the EU (Ireland, Sweden, Germany, Austria, France, Netherlands, Denmark, Finland) and different third countries (e.g. US, UK, Canada, Australia, India, Israel, Japan, Serbia, China, Switzerland, South Africa, United Arab Emirates, Chile, Hong Kong, Brasil, Egypt, South Korea, Singapore, Malaysia) which '*may process, store, or otherwise access'* or '*be exposed to customer data or personal data*'.

Europol argues that the order placed by DG-DIGIT as the broker on behalf of multiple EUIs (Direct Contract 2020-9906) states that its data remains at rest and in transit in the territory

---

- *Appendix I to this SLA contains the list of services provided by the Contractor and centrally maintained by the Paying Entity, services processing personal data. This lists evolves over time as Contractor continues to provide up-to-date information. Entries are duly time-stamped and include:*
  - *the location(s) of the data,*
  - *subject matter of the processing,*
  - *nature and purpose of the processing,*
  - *type of personal data processed and categories of data subjects,*
  - *whether such services are compliant with Chapter V of Regulation (EU) 2016/679 ("GDPR") and of Regulation (EU) 2018/1725 and if so which safeguards are in place.*
- *Appendix I to this SLA contains the list of services provided by the Contractor and centrally maintained by the Paying Entity, services not processing any personal data. This lists evolves over time as Contractor continues to provide up-to-date information. Entries are duly time-stamped and include:*
  - *the location(s) of data,*
  - *subject matter of the processing,*
  - *nature and purpose of the processing,*
  - *type of data processed.*

For services compliant with the requirements of Chapter V of Regulation (EU) 2016/679 ("GDPR") and of Regulation (EU) 2018/1725, the Contracting Authority may require evidence of compliance throughout the duration of the Contract.

3.2.4 Services not processing the customer's data that may be performed outside the European Economic Area
Pursuant to Article 11.3 of the Direct Contract the following supporting services, not processing the customer's data, may be performed outside the European Economic Area:
Appendix I to this SLA contains the list of services maintained by the Paying Entity, managed centrally by the Paying Entity and that evolve in time.
Entries are duly time-stamped and include:
- *the location(s) of performance of the service,*
- *nature and purpose of the services.'.*

[54] See e.g. pages 6 to 9 of that document.
[55] See e.g. page 9 of that document.
[56] See page 10 of that document.

of the European Economic Area. Europol's systems in Azure are in the EEA (Netherlands for the main PERCI infrastructure and Ireland for the backups).

In more detail, according to the information provided by Europol with regard to subprocessors that may have access to PERCI data[57], Europol notes the following:
(i) All data in transfer is encrypted so even if data passes through a subprocessor, the latter does not have visibility over the data;
(ii) With regard to Multi-factor Authentication in Azure, this is only used for Europol staff with an Azure user since Member States use EPE's 2 factors authentication so this is not applicable to the production environment. For the rest of the environments, following the Data Protection Function's advice, Europol uses anonymized user accounts to the extent possible (only using name without surnames);
(iii) With regard to the Azure datacentres selected for PERCI, all data is encrypted with Europol Keys and hence the subprocessors should not have visibility over the data.

Furthermore, according to information provided by Europol orally in the meeting of 15 June 2022, Europol will use the Customer Lockbox solution to authorise access to customer data by the provider or its sub-processors only in case Europol requests support, in which case Europol would give access only to relevant snippets of logs that the provider or the sub-processor needs to troubleshoot the specific issue.

Based on the above, the EDPS considers for the reasons analysed below that the operation of PERCI will entail the transfer of different sets of personal data to different third countries, transfers that were not assessed by Europol.

1. According to the notification of the prior consultation, data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption that cannot be disabled. Europol further clarified [58] that the key management in the Europol Azure Tenant is done by leveraging the Azure KeyVault Premium with HSM (Hardware Security Module) service and customer managed keys capability. It is planned that Europol will deploy customer managed keys for all data-at-rest encryption in the Cloud environment before the go-live. The project team has also assessed the BYOK (Bring-Your-Own-Key) approach, which was discarded as it was not feasible to be applied within the project timeframe (deadline 7 June 2022). Europol does not currently have an Azure compatible HSM to generate its own keys. The key usage on the system is designed to allow a future migration to Europol generated keys once a suitable HSM is available to generate them.

   Europol has thus opted for the customer-managed key solution offered by Microsoft. However even in this case and even for personal data stored in the EEA, the fact that the keys would be saved in the Azure cloud would allow Microsoft to access the keys in response to an order or request for access from US or third country public authorities. The

[57] Draft EDOC # 1228993 v.1.
[58] EDOC#1224686v20, p. 8, under 2.4.

EDPS recalls that US data importers that fall under Section 702 of the Foreign Intelligence Surveillance Act (FISA) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible[59].

Concluding, encryption solutions that do not give to Europol the sole control of the encryption keys do not prevent possible transfers to private parties in third countries outside the scope of Article 26 ER (as in force and as amended by Regulation 2022/991).

2. With respect to the use of Customer Lockbox, the EDPS notes that its use does not eliminate transfers, as access, even limited access (whether in scope or in duration) by a provider or sub-processor from a third country to personal data stored in the EEA is still considered an international transfer of data. It is also unclear to the EDPS what information is provided to Europol in the approval request or what the Europol's options are should they do not wish to approve the access. If the consequences of refusing an access request are that the system will not work or will work only with reduced functionalities, Europol may have no real choice but to approve access. For the abovementioned reasons Customer Lockbox and logging are not eliminating transfers.

3. With regard to Multi-factor Authentication in Azure, the data transferred is pseudonymised and not anonymised, hence limited (in scope) international transfers also take place.

In view of the above, **the EDPS considers that there are possible data transfers to private parties in third countries acting as processors stemming from the use of cloud services. This creates risks of non-compliance with Articles 25 and 26 of the Europol Regulation.**

This issue will not be remedied by the entrance into force of the amended Europol Regulation and the data transfers mentioned above **will create the risk of non-compliance with Article 94 EUDPR and Articles 25 and 26 of the amended Europol Regulation**.

The EDPS thus recommends that Europol further assesses the transfers that the use of cloud services may entail and **eliminates any transfers of operational data.**

[59] See paragraphs 81, 84, 94 and 95 of the EDPB Recommendations 01/2020.

3.4.2.3. Risks stemming from the development and testing of PERCI application with personal data

In previous consultations, EDPS made Europol aware of the data protection risks stemming from using personal data for testing purposes. According to the principles of purpose limitation, data minimisation and the principle of data protection by design and by default (Articles 28(1)(b)(c) and 33 of Europol Regulation[60]), the use of personal data in development and pre-production environments, or any other testing environment, should be avoided where possible as it creates risks for the fundamental rights and freedoms of the data subjects[61].

Originally in the PERCI notification, Europol planned to perform development, testing, verification and validation exclusively with dummy data[62]. In the 'update to the prior notification'[63], Europol informed the EDPS that PERCI development was ceased on 10 May 2022 when Europol 's Data Protection Function found that developers did process personal data from publicly available resources for development and testing, namely with respect to so-called Fetchers [64].

Europol has identified the need for processing personal data from publicly available resources and operational data for development and testing purposes as follows:

- Personal data from publicly available resources: The PERCI production system will interact with public internet sites that include personal data, with HSPs, with Europol and with the Member State authorities. To guarantee a proper functioning of the software it is necessary to test a broad range of URLs, especially with a view to the need of customisation to each of them. Therefore, the exclusive use of dummy URLs is limited and exposes Europol to the risk of not identifying a sufficient number of use cases potentially leading to buggy software. Europol explained that the software must be tested also with real URLs. Ideally, these URLs do not contain personal data. Europol tries to mitigate the risks of using URLs containing personal data upfront (for example by choosing URLs of sites that are not expected to process personal data). However, it cannot be guaranteed that, unintentionally, there are URLs chosen for testing that do contain personal data.

---

[60] Articles 28 and 33 are deleted by Regulation 2022/991. The processing of personal data by Europol as of 28 June 2022 will be regulated by Article 3 and Chapter IX EUDPR, hence by Articles 71 (Principles relating to the processing of operational personal data) and 85 EUDPR (data protection by design and by default), which reinforce the principles provided in Articles 28 and 33 of the Europol Regulation.

[61] Refer as well to EDPS Guidelines on the protection of personal data in IT governance and IT management of EU Institutions, recitals 76-86.

[62] EDOC#1214010, Q4.

[63] EDOC#1231556v7.

[64] Fetchers are pieces of code that replicate the actions of a human interacting with a URL/website, for example:
- Open Browser and navigate to URL;
- Take a screenshot of the illegal content of the URL and save it in a file;
- Check if the content is still available.

- Operational data: Due to the different ways HSPs process removal orders (see section 2.2 on removal orders and the data flow in PERCI), there are different ways to assess if the content has really been removed. The developers must determine URLs that are subject to removal orders (operational data) and test the proper functioning on these cases.

Given that hundreds or even thousands of URLs will have to be assessed it is not feasible to run these processes manually to meet the requirements laid down in Regulation (EU) 2021/784 (one hour for removal orders). However, Europol claims that this will not lead to automated decision-making if the removal order has been performed (i.e. there is no process of making a decision by automated means without any human involvement).

During the meeting with the EDPS on 09 June 2022, Europol explained that regarding the testing they have been using non personal data or dummy data for the majority of the use cases (between 90 and 99%). Europol pointed out that they are committed to keeping the cases to a minimum in which personal data and/or operational data are necessary. Moreover, Europol explained that they established further controls to ensure a sufficient level of data protection, such as data protection e-learning courses for developers, regular deletion of data gathered during development and testing as well as deletion of the database used for development purposes after the go-live of PERCI.

Moreover, Europol claimed in the meeting with EDPS on 9 June 2022 that their policy for testing is directed to data minimization, meaning that Europol is following the rational of not using personal data, but only exceptionally and if needed and there is no alternative means for the testing of the system to use the minimum necessary data. They also follow the rule that in case personal data is used for testing, the necessary security rules are applied and the data is deleted if not necessary for additional services.

In this specific case of PERCI, the EDPS is satisfied that, in certain circumstances, the purpose cannot be achieved reliably with alternative means and without using personal data and operational productions data. Thus, the processing is not in breach of the Europol Regulation (Articles 28(1)(b)(c), 32 and 33).

The EDPS recommends that Europol:

- for **this processing, in the exceptional circumstances described for the specific cases, develops** a **specific policy on this exceptional use** including all the necessary safeguards followed by all staff exceptionally for the PERCI system **and documents** its application;
- **keeps the use** of personal and operational data for development and testing **to a minimum** and closely monitors the effectiveness of the safeguards;
- after the go-live of the PERCI system, **Europol confirms to the EDPS deletion** of all personal and operational data from development and testing environments.

3.4.2.4. Risks stemming from the lack of an adopted Cloud Strategy

The EDPS notes that so far Europol provided solely draft documents on its cloud strategy and the related security strategy, the earliest stemming from January 2020. The EDPS cannot determine an approach on cloud computing approved by senior management explaining the necessity to go to the cloud and how data protection risks and security threats are planned to be addressed.

In the absence of a strategic planning underpinning the move to the cloud there is the risk that the move of PERCI to the cloud may be ad-hoc and without a comprehensive assessment of the consequences of such a choice, also as to data protection implications. This may cause the set of data protection safeguards being not sufficiently founded and thus potentially leading to gaps. This may result in personal data breaches putting the rights and freedoms of the data subjects at risk.

The EDPS **recommends that Europol finalises its cloud strategy** including **a cloud computing security and data protection policy**. This document should explain the necessity of migrating to the cloud. The Data Protection Impact Assessment and its consequences should then be verified based on the conclusions made in the cloud strategy.

4. CONCLUSION AND RECOMMENDATIONS

Based on all of the above, the EDPS is of the view that Europol has insufficiently identified the specific risks related to the development and operation of PERCI. As a consequence, the EDPS **recommends that Europol**:

- Ensures that, with regard to the assignment of the processing of operational data to a processor (which is a private party), the contractual framework binds the latter to meet the requirements of the Europol Regulation and as of 28 June 2022 of Chapter IX EUDPR as specified by the amended Europol Regulation. This could take place either in or outside the context of the respective Cloud II framework contract.

- Further assesses the international transfers that the use of cloud services may entail and eliminates any transfers of operational data to private parties in third countries acting as processors;

- Develops a specific policy on the exceptional use of personal data for the development and testing of PERCI and documents its application;

- Keeps the use of personal and operational data for development and testing to a minimum and closely monitors the effectiveness of the safeguards;

- Confirms the deletion of all personal and operational data from development and testing environments after the go-live of PERCI;

- Finalises its cloud strategy, which should include a cloud computing security and data protection policy.

Done at Brussels on 27 June 2022

[e-signed]

Wojciech Rafał WIEWIÓROWSKI