

CM2405

COMMENT ON EUROPOL'S DATA SUBJECT CATEGORISATION BASED ON THE AMENDED EUROPOL REGULATION

MAY 2024

Europol's increased personal data processing powers have included and still include powers to process personal data that does not have a 'data subject categorisation'. This is an indication of the status of the person to whom the data refers, be it suspect, victim, witness, etcetera. Such indications are important to limit the processing of personal data to what is necessary and proportionate, and to safeguard fundamental freedoms and legitimate interests of all citizens in the European Union. Indeed, data subject categorisation is one of the most important tools to protect the right to protection of personal data in criminal proceedings. In line with consistent standpoints of the European Data Protection Supervisor and Court of Justice case law, the Meijers Committee strongly recommends to significantly limit and provide further safeguards to this aspect of Europol's data processing, and also calls to Member States to assist Europol in this.

1. Introduction to amendment: expanding Europol's personal data processing powers

The 2022 amendment¹ of the Europol Regulation² endowed the European Union Agency for Law Enforcement Cooperation (further: Europol) with unprecedented extensive personal data processing powers and operational capacities. Under its overhauled legal framework, Europol is allowed to collect more personal data than before from a number of partners, as well as exchange these data with them.³ These partners include Member States, EU bodies, third countries, international organizations, and even private parties.⁴

Europol is also competent to process these personal data more widely than before, thanks to both the extension of Europol's information processing purposes⁵ and the more extensive possibilities given to Europol to develop and use far-reaching investigation and data processing tools based on state-of-the-art digital technologies and algorithms.⁶ Europol's expanded information-related powers and operational capacities are said to contribute to more effective EU law enforcement. These powers would allow better support to Member States in a context in which both national enforcement authorities and the EU at large are confronted with novel and serious security threats, such as terrorism and large-scale cyber-attacks.⁷

At the same time, these strengthened Europol capacities raise important legal questions and concerns about the proper safeguards put in place to ensure that Europol's extended powers are subject to sufficient conditions, oversight and control, so that the rule of law and fundamental rights are preserved alongside enhanced operational effectiveness considerations.⁸ These safeguards follow from not only the right to private life and data protection as protected in Article 7 and 8 of the EU Charter on Fundamental Rights, but also the Directive 2016/680 concerning data processing within the context of law enforcement. The Meijers Committee stressed the importance of these safeguards in a comment on the proposal, published in October 2021.⁹

2. Processing personal data without a data subject categorisation

¹ 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, OJ L 169, 27.6.2022, p. 1–42.

² 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.

³ Regulation (EU) 2016/794 (consolidated text).

⁴ See on the relationship between Europol and private parties, Articles 26, 26a, 26b and 27 Regulation (EU) 2016/794 (consolidated text).

⁵ See Article 18 (2), in particular amended (d) and newly introduced (e) and (f) Regulation (EU) 2016/794 (consolidated text).

⁶ See Articles 2 (v) and 33a Regulation (EU) 2016/794 (consolidated text).

⁷ See Recitals (2)-(5) to the Preamble of Regulation (EU) 2022/991.

⁸ See generally, Jane Kilpatrick, Chris Jones. Empowering the police, removing protections: the new Europol Regulation (Statewatch, November 2022), and pp 8-11 regarding specifically personal data processing by Europol. See recently on Europol' liability for damages caused breaches of fundamental rights as a result of unlawful processing of personal data of suspects in the context of criminal investigations, Case C-755/21 P. *Kočner v European Union Agency for Law Enforcement Cooperation* ECLI:EU:C:2024:202.

⁹ Meijers Committee comment CM2114, Comment on Proposed Extensive Data Processing Powers for Europol, October 2021, to be found at: https://www.commissie-meijers.nl/wp-content/uploads/2021/10/CM2114_EN.pdf.

With the current comment, the Meijers Committee wants to comment on one particularly controversial issue that stems from the legal design and implementation of the amended Europol Regulation. This concerns Europol's powers and its practice to collect, process and retain large personal datasets which lack a 'data subject categorisation' (DSC) according to Article 18 and Annex II of Regulation (EU) 2016/794. Requiring such a data subject categorisation is a way to give effect to the principle of data minimisation, a central principle in the protection of personal data. It provides attributes that can inform authorities of how to process particular data and to limit the processing of particular data to what is necessary and proportionate. Therefore, a data subject categorisation helps in obtaining the objectives of data protection law, while not disproportionately restricting operational use.¹⁰

Annex II to the Europol Regulation specifies the categories of persons whose personal data are processed by Europol for the purpose of analysis of a strategic or thematic nature, for operational analysis or for facilitating the exchange of information between Member States, Europol, other EU bodies, third countries and international organisations.¹¹ The Regulation differentiates between six categories: (a) suspects or convicted persons; (b) persons who are likely going to commit an offence; (c) witnesses; (d) victims; (e) contacts and associates; (f) informers.

This distinction between the different categories of persons whose data is processed by Europol is legally relevant, as the amended Europol Regulation, requires, in Article 18(5a): "In accordance with Article 73 of Regulation (EU) 2018/1725 of the European Parliament and of the Council, Europol shall, where applicable and as far as possible, make a clear distinction between the personal data that relate to the different categories of data subjects listed in Annex II." However, currently Europol continues to process large datasets of personal data that lack a DSC.

3. EDPS involvement in Europol's data processing

This issue was the focus of the so-called 'Europol's Big Data Challenge', entailing an inquiry on the own initiative of the European Data Protection Supervisor (EDPS) on large datasets lacking a DSC in Europol's forensic environment, followed by an EDPS decision finding that the processing of those datasets by Europol constituted a breach of the Europol Regulation. This led the EDPS to admonish the Agency,¹² and culminated in a second EDPS decision imposing on Europol specific data retention periods for datasets lacking a DSC.¹³

In essence, the EDPS concluded that Europol's continuous storing and processing (without clear conditions and limits) of large personal datasets concerning individuals with regard to whom it is uncertain whether they belong to one of the categories whose personal data can be processed under the Europol Regulation did not comply with Article 18 of that Regulation (before the 2022 amendment) and with the data minimization principle. The EDPS highlighted in particular the serious interference of such extensive data processing by the Agency with data protection and other fundamental rights of data subjects, such as damage to their private and family life, freedom of movement and occupation.

¹⁰ European Data Protection Supervisor (EDPS) Decision of 21 December 2021 on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699), point 4.5.

¹¹ Europol Regulation, Annex II, under B(1)(a)-(f).

¹² European Data Protection Supervisor (EDPS) Decision of 17 September 2020 on the EDPS own initiative inquiry on Europol's big data challenge (case 2019-0370).

¹³ European Data Protection Supervisor (EDPS) Decision of 21 December 2021 on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699).

These could be affected because the persons concerned run the risk, across the EU, of being wrongfully linked to a criminal activity.¹⁴

4. Amended legal framework

Yet, despite these already existing concerns by the EDPS, the legislator continued with extending the data processing powers of Europol. Last-minute amendments were included in Regulation 2022/991 concerning the processing of personal data without DSC by Europol. First, Europol is enabled to carry out a pre-analysis, without further analysing them, of personal data received in the context of preventing and combating crimes that fall within its objectives for the sole purpose of establishing whether they relate to one of the categories of data subjects listed in Annex II of the amended Europol Regulation,¹⁵ The Agency may process personal data to that effect for a period of up to 18 months from the moment Europol ascertains that those data fall within its objectives or, in justified cases, for a longer period not exceeding 3 years.

Second, the amending Regulation provides for a new legal basis for Europol's processing of large datasets without DSC in support of criminal investigations.¹⁶

Third, and more controversially, these amendments retroactively validate the processing of such datasets by Europol in the past, before the entry into force of the 2022 Amending Regulation.¹⁷ Thereby, they effectively counteract the EDPS's decision imposing on Europol specific data retention periods for datasets lacking a DSC.

5. Further EDPS involvement and responses

In December 2022, the EDPS carried out an audit of Europol, including an inspection which specifically targeted Europol's processing of personal data of suspects below the age of majority.¹⁸ The EDPS found that Europol is confronted with varying requirements relating to DSCs: when it receives personal data from Member States, these are the ones that are responsible for providing a DSC, while Europol itself is responsible for that when it receives personal data from third countries or international organisations. Furthermore, the EDPS noted that processing all personal data of persons who have been labelled as 'suspects' in the same manner may be disproportionate, as some suspects only have minor roles in, for instance, a criminal organization, compared to other suspects.

Earlier, on 17 November 2022, the EDPS issued an Opinion regarding four draft decisions by which the Europol Management Board (EMB) intended to implement Article 18(2), Article 18(6), Article 18(6a) and Article 18a of the revised Europol Regulation.¹⁹ In its Opinion, the EDPS raised important concerns

¹⁴ European Data Protection Supervisor (EDPS) Decision of 17 September 2020 on the EDPS own initiative inquiry on Europol's big data challenge (case 2019-0370) p. 7 and EDPS Decision of 21 December 2021 on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699) p. 11.

¹⁵ Article 18(6a) Regulation (EU) 2016/794 (consolidated text).

¹⁶ Article 18a Regulation (EU) 2016/794 (consolidated text).

¹⁷ Articles 74a and 74b Regulation (EU) 2016/794 (consolidated text).

¹⁸ European Data Protection Supervisor (EDPS), Audit Report on the European Union Agency for Law Enforcement Cooperation (Europol), The Hague, 16 December 2022, EDPS Case number 2022-0382.

¹⁹ European Data Protection Supervisor (EDPS), SUPERVISORY OPINION ON EUROPOL'S MANAGEMENT BOARD DECISIONS ADOPTED PURSUANT TO ARTICLES 11(1)(q), 18 AND 18a OF THE EUROPOL REGULATION, Brussels, 17 November 2022, EDPS Case number 2022-0923.

regarding in particular the way in which the EMB interpreted Article 18(6a) and Article 18a and intended to ensure their implementation.

After receiving the EDPS's opinion, the EMB adopted the four decisions implementing Article 18(2),²⁰ Article 18(6),²¹ Article 18(6a)²² and Article 18a²³ of the amended Europol Regulation. In particular the two decisions pertaining to the implementation of Article 18(6a) and Article 18a, addressed only in part the concerns and issues raised by the EDPS in its opinion. Meanwhile, the decision by the EU legislator to include a new legal basis for Europol's processing of large datasets without DSC, and to retroactively validate previously received personal data, caused uproar with the EDPS, who started a procedure before the General Court to ask for the annulment of the newly introduced Articles 74a and 74b of the Europol Regulation. The General Court however declared the action inadmissible.²⁴

6. Status quo

Against this background, the matter remains unsettled. There is a significant chance that the way in which the provisions in the amended Europol Regulation regarding the processing of datasets lacking a DSC are currently being implemented by Europol does not sufficiently take into account the importance of maintaining a distinction between the categories of persons whose data are processed, as well as the specific safeguards and limitations required by the processing of personal data without DSC in view of their particularly intrusive effects on data subjects' fundamental rights.²⁵ After all, such a practice would reflect Europol's wishes as to the conditions for processing and data retention of such data.²⁶

Most importantly, the current versions of the Europol Management Board's decisions implementing Articles 18(6a) and 18a fail to reflect sufficiently the EDPS's recommendations regarding in particular, the need to:

- (a) to clarify the term of 'erasure' of personal data;
- (b) define the term 'specific criminal investigation' of the purpose of implementing Article 18a;
- (c) establish specific criteria for assessing when it is not possible to support the specific criminal investigation under Article 18a, without processing personal data without DSC;
- (d) establish a procedure and criteria enabling to select which data should be further stored in order to ensure the veracity, reliability and traceability of the criminal intelligence process under Article 18a;

²⁰ Management Board Decision further specifying procedures for the processing of information for the purposes listed in Article 18(2) of the Europol Regulation of 21 March 2023 (EDOC#1252127v8A).

²¹ Management Board Decision on the conditions related to the processing of personal data on the basis of Article 18 (6) of the Europol Regulation of 21 March 2023 (EDOC#1252123v8A).

²² Management Board Decision on the conditions related to the processing of personal data on the basis of Article 18 (6a) of the Europol Regulation of 21 March 2023 (EDOC#1252125v10A).

²³ Management Board Decision on the conditions related to the processing of personal data on the basis of Article 18a of the Europol Regulation 21 March 2023 (EDOC#1252126v9A).

²⁴ General Court 6 September 2023, Case T-578/22, ECLI:EU:T:2023:522. The European Data Protection Supervisor (EDPS) has lodged an appeal against the GC Order declaring EDPS's action inadmissible before the CJEU - Case C-698/23 P EDPS v Parliament and Council lodged on 16 November 2023 (pending).

²⁵ See European Data Protection Supervisor (EDPS) Case number 2022-0923 para. 14.

²⁶ European Data Protection Supervisor (EDPS) Decision of 21 December 2021 on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699) p. 4-5 and 7.

(e) establish concrete criteria to determine the precise period, within the general limit of 18 months in Article 18(6a), for processing and storing data without DSC in specific cases;

(f) establish concrete criteria under Article 18(6a) to justify the necessity of prolonging a storage period beyond 18 months, and to reflect that the extension to the maximum period of three years is lawful only when it is necessary and proportionate and not when it only facilitates compliance with Article 18(5);

(g) adopt concrete technical and organisational measures ensuring the functional separation of the non DCS data processed.²⁷

Currently, there seems to be little to no development in this file, and the decisions of the Europol Management Board appear to remain unchanged, not addressing the recommendations of the EDPS that point out which particular improvements need to be made. This means that the combined practices of Member States and Europol to exchange and process personal data without sufficient data subject categorisations continue without sufficient safeguards and/or limitations.

7. Normative framework

In a recent judgment, the Court of Justice of the European Union (CJEU) stressed the importance of safeguarding the rights to privacy and data protection in the context of criminal proceedings. It considered that the storage of personal data “constitutes an interference with the fundamental rights to respect for private life and to the protection of personal data, irrespective of whether or not the information stored is sensitive, whether or not the persons concerned have been inconvenienced in any way on account of that interference, or whether or not the stored data will subsequently be used.”²⁸

Such an interference must have a legal basis and might be justified, but to that end, an elaborate system of safeguards must be designed that is laid down in very detailed rules and regulations, which for the case of Europol are contained in the Europol Regulation. However, that is not the only source that calls for a DSC, because this is also a prominent requirement in Directive 2016/680 (Law Enforcement Directive), which is directed at the Member States who are, in respect to data processing by Europol, responsible for providing personal data with a categorisation when sending it to the Agency.²⁹

Data subject categorisation is one of the most important tools to protect the right to protection of personal data in criminal proceedings, according to Directive 2016/680. The preamble to Directive 2016/680 indicates categories such as suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals.³⁰

²⁷ See European Data Protection Supervisor (EDPS) Case number 2022-0923.

²⁸ Court of Justice 30 January 2024, Case C-118/22 (NG), para. 42.

²⁹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *OJ L 119, 4.5.2016, 89–131.*

³⁰ Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

More concretely and, moreover, of a binding nature, is Article 6 of the Directive. This instructs the Member States to provide for the controller, where applicable and as far as possible, to make a clear distinction between four categories of persons concerned (concisely put: suspects, convicted persons, victims and witnesses).

8. A shared challenge

Thus, Europol and the Member States are under a shared legal obligation to make sure that the processing by Europol of personal data in the context of criminal proceedings takes place in a way that the requirements of data subject categorisation are fully respected. In view of the reasoning of the Court of Justice, the processing of personal data lacking a DSC constitutes such an intrusive interference with the right to personal data protection and the data subject's fundamental rights, that it is difficult to justify, and likely will be unlawful.

9. Recommendations

The Meijers Committee therefore recommends:

- Member States and third countries should provide by default a 'DSC' to the personal data sent to Europol, so that the application of Articles 18(6a) and 18a Europol Regulation becomes exceptional in practice, in line with the intention of the Europol Regulation.
- Europol should refuse in principle to process personal data without DSC, unless the data provider duly justifies that assigning a DSC was not objectively possible. Europol should insist upon data providers to provide data with a DSC in all cases.
- For personal data lacking a DSC that is already received by Europol, the data provider should assign a DSC within a reasonable time, and suspend data processing operations pending the response of the data provider. Europol should assist with this process.
- In the exceptional situation where Europol processes personal data without DSC under Articles 18(6a) or 18a, it must ensure that it limits processing to what is strictly necessary and proportionate (to duly document and justify this with the EDPS) in line with purpose limitation, data minimization, and storage limitation principles, and with due observance of data subjects' fundamental rights, in particular the rights to privacy and data protection.
- Europol should further amend its decisions implementing Articles 18(6a) and 18a, in light of the EDPS Opinion of 17 November 2022, to fully comply with the Europol Regulation and fully reflect the exceptional and restricted nature of the processing of personal data lacking a DSC, in line with applicable (data protection) principles and with due observance to the data subjects' fundamental rights.

and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016, L 119/89, recital 31.

About

The Meijers Committee is an independent group of experts that researches and advises on European criminal, migration, refugee, privacy, non-discrimination and constitutional law.



post@commissie-meijers.nl



+ 31 20 362 05 05



commissie-meijers.nl



[Twitter](#)



[LinkedIn](#)