EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorisation

(Cases 2019-0370 & 2021-0699)

1. Introduction

1.1. This Decision concerns Europol's retention policy for the storage and deletion of datasets lacking a Data Subject Categorisation ('DSC').

1.2. This Decision follows from the EDPS own initiative inquiry on large datasets lacking a DSC processed in Europol's forensic environment, and its compliance with Article 18(3), 18(5) and Annex II.B of Regulation (EU) 2016/794[1] ('the Europol Regulation', or 'ER' abbreviated). The Decision results from the follow-up to the EDPS Decision[2] and admonishment of 17 September 2020 on Europol's processing of large datasets (referred to as 'Europol's Big Data Challenge.')

1.3. Large datasets are defined as datasets which, due to the volume, nature or format of the data they contain, cannot be processed in the Europol Operational Network ('OPS NET').

1.4. Large datasets 'lacking a DSC' refer to datasets which, because of their characteristics and notably their size, did not undergo the data classification process as provided for in the Europol Regulation (the so-called 'data subjects categorisation' or 'DSC') and extraction of data categories according to Annex II B ER and the Opening Decision Orders, which specify, for each operational analysis project, the categories of personal data and categories of data subjects that can be processed according to Article 18(3)(a) ER.

1.5. The EDPS issues this Decision based on Article 43(3)(e) ER.

---

[1] Regulation 2016/794 of the European Parliament and 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, 24.05.2016.

[2] 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).

2. Background

EDPS own-initiative inquiry on Europol's Big Data Challenge

2.1. On 30 April 2019, the EDPS decided to open an own initiative inquiry on the use of Big Data Analytics by Europol for purposes of strategic and operational analysis (case 2019-0370). The evolution of Europol's personal data processing activities towards forms of 'Big Data Analytics' raised concerns linked to the compliance with the applicable data protection framework, in particular with the principles of purpose limitation, data minimisation, data accuracy, storage limitation, with the impact of potential data breaches, location of storage, general management and information security.

2.2. On 17 September 2020, the EDPS concluded his investigation and issued an admonishment to Europol, on the basis of his findings that the processing of large datasets did not comply with Articles 18(3), 18(5) and Annex II.B of the Europol Regulation, as well as the principle of data minimisation (Article 28(1)(c) of the Europol Regulation).

2.3. The EDPS considered that Europol, as data controller, was in a better position to devise mitigation measures that would both reduce the risks for data subjects and ensure that Europol does not lose its operational capabilities. The EDPS therefore considered that imposing an order of erasure of personal data or a ban, pursuant to Article 43(3)(e) and (f) of the Europol Regulation would, at that time, not have been appropriate.

2.4. However, in view of the high risks for data subjects and potentially severe impact on their fundamental's rights and freedoms, the EDPS urged Europol to implement all necessary and appropriate measures to mitigate the risks created by such personal data processing activities to data subjects. He invited Europol to provide an action plan to address the admonishment within two months and to report on the measures taken within six months.

Europol Action Plan and follow-up to the EDPS Decision and admonishment on Europol's big data challenge

2.5. On 17 November 2020, Europol sent an Action Plan[3] detailing Europol's measures to address the risks raised in the EDPS Decision. The Action Plan set out five categories of measures intended to strengthen Europol's data review activities and build enhanced controls into the New Forensic Environment ('NFE'), i.e. the new operational environment foreseen to replace the Computer Forensic Network ('CFN') as the technical platform for handling large datasets:

(1) the flagging of large datasets lacking DSC in SIENA by the data provider;

[3] Europol Action Plan of 17 November 2020 addressing the risks raised in the EDPS Decision on 'Europol's Big Data challenge,' EDOC#1131384v14A.

(2) the labelling of these datasets in Europol's environment before the start of the extraction process;

(3) the definition of strict access rights in order to limit access to these datasets only to the persons in charge of performing the extraction process;

(4) the implementation of quarterly reviews in order to assess whether the large datasets which have not been through the whole extraction process should be retained or deleted;

(5) the appointment of a Data Quality Control Coordinator in order to closely monitor the data review process.

2.6. On 4 December 2020, the EDPS provided comments on the Action Plan, and requested further clarifications on a number of elements. Among these, the EDPS expressed reservations regarding the efficacy of the review process of large datasets lacking a DSC and requested more information regarding the time limit to be put on the fulfilment of the extraction task. The EDPS also asked for clarifications regarding the exact content of the review performed by the analysts/specialist of the Analysis Project ('AP') at the level of extraction, and the policy applied by Europol regarding deletion, i.e. whether the raw data are deleted once the relevant data have been extracted.

2.7. The EDPS stated that he considered that the review process under Action 4 should be stricter and contain clear criteria, for instance by imposing a maximum time limit for the storage of these large datasets, as there is no guarantee that these datasets are processed in line with the restrictions of Annex II.B ER.

2.8. On 17 March 2021, Europol sent a Progress Report[4] detailing the state-of-play concerning measures being put in place under the Action Plan. In the Progress Report, as regards the question of whether Europol will define a maximum retention period for datasets pending a DSC, Europol states that it will "*keep the data for as long as is necessary and proportionate for the support to the investigation concerned.*"[5]

2.9. On 19 April 2021, the EDPS sent a letter to Europol commenting on the progress report and expressing serious concerns relating to data minimisation and retention of datasets lacking a DSC. In particular, the EDPS noted that Europol had not specified a time limit for the extraction process or a maximum retention period for datasets lacking a DSC. The letter instructs Europol to define and put in place a maximum retention period for datasets lacking a DSC, beyond which datasets must be deleted, and to do so with immediate effect[6].

2.10. On 2 June 2021, Europol replied to the EDPS.[7] As regards the request to implement a maximum retention period for datasets without a defined DSC, Europol re-stated that the datasets will be subject to increased reviews to determine the necessity and proportionality

[4] Europol Progress Report of 17 March 2021 on the Europol Action Plan addressing the risks raised in the EDPS Decision on 'Europol's Big Data challenge,' EDOC#1156601v13A.

[5] Ibid, p. 12.

[6] "*The EDPS requests Europol to implement a maximum retention period for datasets lacking a DSC. Once that retention period is exceeded, datasets lacking a DSC must be deleted. The EDPS requests that the new retention policy concerning large datasets pending a DSC be implemented as of receipt of this letter, and procedures and guidance to staff be updated accordingly*" EDPS letter D(2021)882 of 19 April 2021, p. 3.

[7] Europol letter of 2 June 2021, file no. 1169084v5B.

of retaining the data for the purpose of an ongoing investigation and to ascertain the time required to determine the DSC when this request comes from a Member State. Europol stated that a default retention period would not be appropriate to its core business and would hamper the success of live investigations.

2.11. By letter of 26 July 2021, the EDPS notified Europol of its intention to set an appropriate retention period for large datasets lacking a DSC, in light of Europol's refusal to do so, and to issue an order to permanently delete those datasets which do not comply. The EDPS also provided a provisional legal analysis of the processing,[8] which drew the preliminary conclusion that a maximum retention period of six months should be applied to the processing of large datasets pending a DSC, after which such datasets should be permanently deleted. The EDPS invited Europol to submit observations or alternative considerations on the provisional analysis and to substantiate them with operational and legal arguments, before taking any enforcement action.

2.12. On 20 October 2021, Europol provided a second progress report on the implementation of the Action Plan,[9] together with a letter providing written observations[10] on the EDPS' provisional analysis of 26 July 2021. In the latter, Europol contends that a retention period of six months would not be sufficient to allow for an adequate analysis of large and complex datasets and refutes the EDPS' interpretation that the Europol Regulation does not provide for the possibility for Europol to process large datasets shared by Member States for purposes of operational analysis, for the sole purpose of extracting relevant information in compliance with Article 18(3), (5) and Annex II B ER.

2.13. Europol considers that processing non-DSC data for the purpose of extracting relevant data in compliance with the ER is included under the objectives, tasks and competences as set out in the ER.[11] According to Europol, the act of reducing, filtering and extracting data for the purposes of criminal intelligence is integral to the activity of law enforcement analysis. Thus, according to Europol, the provisions under Articles 31 and 28 ER and the principles of necessity and proportionality apply to the processing of operational personal data, including the applicable retention period.

2.14. Europol acknowledges that in the absence of an explicit legal provision laying down a retention period for large datasets lacking a DSC, there is a need to find a solution that "better meets, on the one hand, the key data protection principles of necessity and proportionality in the interests of data subject rights, and on the other hand, the operational core business needs of Member States and Europol."[12] Consequently, and taking note of the ongoing legislative process to amend the Europol Regulation, Europol requested the EDPS to:

[8] EDPS letter D(2021)1636 of 26 July 2021.
[9] Europol Progress Report of 19 October 2021 on the Europol Action Plan addressing the risks raised in the EDPS Decision on 'Europol's Big Data challenge,' EDOC#1176446v14A.
[10] Europol letter of 20 October 2021, EDOC#1191646v7B.
[11] Ibid, p.8-9.
[12] Ibid, p.6.

1) Defer a decision on whether to issue an order to delete until the proposed Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794[13] enters into force;

2) In the meantime, agree to Europol's implementation of a retention period that aligns with the 'minimum common denominator' expressed in the current legislative process by the respective positions of the co-legislators.[14] As proposed by Europol, this retention period would allow Europol to store large datasets where the DSC is not completed for a period of twelve months, extendable by up to a further six months in duly justified cases, where further processing is necessary and proportionate. This retention period would not apply to personal data collected within the context of a specific ongoing criminal investigative case supported by Europol (e.g. a Joint Investigation Team or Operational Task Force). In such cases, Europol proposes that the processing without a defined DSC would be performed for as long as Europol supports the on-going specific criminal investigation.

3. Findings of facts

Mitigation actions for the processing of large datasets pending a DSC in Europol's forensic environment

3.1. Under the Action Plan responding to the EDPS admonishment on Europol's big data challenge, a number of technical controls are being implemented in the Secure Information Exchange Network Application ('SIENA'), the NFE (CFN's successor) and integrated into the new data environment, to mitigate the risk that data without a DSC is processed or integrated into Europol's analysis work.

3.2. An update of Europol's SIENA has been put in place making it mandatory for those contributions pending a DSC to be flagged by the contributor to indicate whether the DSC is 'Completed', 'Not Completed' or 'Not applicable.'

3.3. Europol performs a second assessment upon acceptance of the contributions. After the second assessment, the following steps are followed:

a) All messages which are accepted with a second assessment of 'DSC Completed', are accepted into the data environment for further processing.

[13] Proposal for a Regulation of the European Parliament and of the Council 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 on research and innovation, COM(2020) 796.

[14] Proposal for a Regulation of the European Parliament and of the Council 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 on research and innovation, (2020/0349(COD)); Report of the LIBE Committee of the European Parliament of 15.10.2021 on the proposal for a regulation of the European Parliament and of the Council 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 on research and innovation, A9-0290/2021.

b) All messages which are accepted with a second assessment of 'DSC Not Completed', are accepted into the data environment but with limited access rights given.

c) All messages which are accepted with a second assessment of 'DSC Not Applicable', are accepted into the data environment if relevant for case management purposes (these messages do not contain personal data).

3.4. In the new data environment, scheduled to replace Palantir in Q3 of 2021 [redacted] all accepted SIENA contributions where the DSC is not completed will be automatically labelled as such and these labels will be visible on the contributions as a file property. All data in the data environment will be accessed via the new [redacted] and the labelling will be clearly visible to those accessing the data. Pending the launch of the new data environment, Europol will put in place a temporary, interim solution for the automatic labelling of new Serious and Organised Crime (SOC) data.

3.5. Specific folders have been created in the CFN (which will be replicated in the NFE) for the storage of data lacking a DSC. Access rights are currently limited in the CFN and will be further limited in the NFE upon its deployment. Europol states that a limited number of designated Europol staff with a dedicated forensic training will be given access to the NFE. It will be their responsibility to liaise with the relevant Analysis Projects in order to identify the DSC and extract the data where the DSC has been identified.

3.6. Europol has confirmed that with the progressive implementation of the above controls, data without a DSC will not be further processed for analysis, included in a Europol analysis product, be subject to a general search against new information received by Europol, or be shared with a Member State or third party.

Extraction, retention and deletion of large datasets lacking a DSC

3.7. As stated in the EDPS Decision of 17 September 2020, it is not possible for Europol, when receiving large datasets, to ascertain that all information contained in these large datasets comply with the limitations in the ER. Due to the volumes of information concerned, their content is often unknown until the moment when the analyst extracts the relevant entities for their input into the relevant database in OPS NET.

3.8. During the extraction, a filtering takes place (data minimisation) based on the restrictions in the respective AP Opening Decision (categories of data subjects, crime area, operational relevance, and in agreement with the data provider according to what is required). Where the DSC is not provided, designated staff work to identify the DSC during the extraction process. The extracted data undergoes another review by the analysts/specialists of the AP, in order to further reduce the amount of data and ensure compliance. Once the data has been properly reviewed, it becomes available and accessible to a larger group of users, via the Unified Search Engine (USE) and the Europol Analysis System (EAS).

3.9. There is no time limit imposed by Europol for the fulfilment of the extraction task. Europol states that once extraction is completed, data where no DSC can be identified is deleted. However, the lack of a deadline for this task means that in principle the extraction process may last years, allowing analysts to return to datasets where extraction has not been officially completed in case of a new lead or new development in the criminal investigation.

3.10. Under the new approach to data review (Action 4 of the Action Plan), Europol keeps a record of the data without a DSC in a Data Quality Logbook and APs review these contributions on a quarterly basis to ensure the necessity and proportionality of their continued retention. This process is overseen by the Data Quality Control Coordinator (appointed under Action 5 of the Action Plan).

3.11. Once it is established that the data is no longer needed for the purpose of an ongoing investigation or for the purpose of determining the DSC, the data is deleted, except where it is stored to preserve the chain of evidence (required to ensure that the data is admissible as evidence in a court of law). According to Europol, datasets retained to preserve the chain of evidence will remain stored in the same secure location as datasets lacking a DSC, be subject to similar access controls (available to the analysts and forensic specialists that have worked on the investigation), and will continue to be periodically reviewed, although no further data will be extracted from it.[15]

3.12. Europol's existing policy for the retention of large datasets lacking a DSC is to store the datasets for "as long as is necessary and proportionate for the support to the investigation concerned"[16]. Europol does not detail the threshold or criteria that it applies to the necessity and proportionality assessment, but explains that gauging the necessity and proportionality of continued storage is subject to an assessment on the merits of the individual contribution.

3.13. Europol has stated that it takes all necessary measures to ensure that this is done in the shortest time possible and in line with the rules on data retention as defined under the Europol Regulation.

3.14. Europol states that a retention period of six months would not be sufficient to allow for the detailed analysis of large and complex datasets that is necessary to determine the DSC. This is due, in part, to the volume of seized material in the field of digital forensics and intercepted communications that Europol receives from Member States.

3.15. Furthermore, Europol contends that a longer retention period is necessary given the nature of operational analysis in the context of long-running criminal investigations, where complementary or new information received in the course of an investigation can render a data item as being related to a specific DSC, although not previously identified in the underlying operational analysis. Europol draws attention to the 2021 SOCTA which highlights that it is a common feature of criminal networks to operate for more than 10 years.[17]

---

[15] Europol letter of 2 June 2021, file no. 1169084v5B, p.4; Europol Progress Report of 19 October 2021 on the Europol Action Plan addressing the risks raised in the EDPS Decision on 'Europol's Big Data challenge,' EDOC#1176446v14A, p.6.

[16] Europol Progress Report of 17 March 2021 on the Europol Action Plan addressing the risks raised in the EDPS Decision on 'Europol's Big Data challenge,' EDOC#1156601v13A, p. 12.

[17] European Union Serious and Organised Crime Threat Assessment (SOCTA), 12 April 2021:

3.16. Based on the above, Europol contends that such an order to erase based on a six month retention period would seriously impair the delivery of objectives and tasks that the legislator assigned to Europol under the ER.

4. Legal analysis

4.1. The processing of datasets which are shared with Europol for purposes of strategic and operational analysis, in accordance with Article 18(2)(b) and (c) ER[18], should comply with the provisions of Article 18(3), 18(5) and Annex II B ER.

4.2. Article 18(3) of the Europol Regulation states that the processing of personal data for the purpose of operational analysis should be performed in compliance with specific safeguards. In particular, the Executive Director must define "the categories of personal data and categories of data subjects ... [the] duration of storage...."

4.3. Article 18(5) of the Europol Regulation limits the categories of personal data and categories of data subjects whose data may be collected and processed for purposes of strategic and operational analysis by Europol as listed in Annex II.B.

4.4. Annex II.B (1) of the Europol Regulation limits the categories of data subjects about whom Europol can process data to 'suspects'[19], 'potential future criminals'[20], 'contacts and associates'[21], 'victims'[22], 'witnesses'[23] and 'informants'[24]. Annex II.B (2), (3), (4), (5), (6) defines which categories of personal data Europol can process in relation to each of the categories of data subjects mentioned above. Europol must not process personal data beyond these categories of data subjects and of personal data.

---

https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

[18] See FITE Use and Management Policy of 30 November 2012, EDOC#506111-v22; DPO Note on DPF Preliminary scrutiny of CFN usage, 15 February 2019, EDOC#1026517, EDPS Annual inspection report of 19 December 2019.

[19] According to Annex II.B(1)(a), these are persons who, pursuant to the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence.

[20] According to Annex II.B(1)(b), these regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent.

[21] According to Annex II.B(3), 'contacts' and 'associates' are persons through whom there is sufficient reason to believe that information which relates to suspects and future potential criminals and which is relevant for the analysis can be gained, provided they are not included in one of the other categories of persons referred to paragraph 1. 'Contacts' are those persons who have a sporadic contact with 'suspects' and 'potential future criminals'. 'Associates' are those persons who have a regular contact with those persons.

[22] According to Annex II.B(1)(d), these are persons who have been the victims of one of the offences under consideration or with regard to whom certain facts give reason to believe that they could be the victims of such an offence.

[23] According to Annex II.B(1)(c), persons who might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings.

[24] According to Annex II.B(1)(e), these are persons who persons who can provide information on the criminal offences under consideration.

4.5. All the provisions mentioned above give effect to the principle of data minimisation for the processing of personal data for operational analysis purposes, as defined under Article 28(1)(c) of the Europol Regulation. They implement the necessary safeguards to limit the processing of personal data to data that are adequate, relevant and limited to what is strictly necessary for the purposes for which they are processed, i.e. for purposes of strategic and operational analysis. These safeguards have been put in place by the EU legislator taking into consideration the specificities of Europol's tasks.

4.6. The Europol Regulation contains a specific set of provisions (Article 18(3), 18(5), and Annex II.B) which are particular to Europol and which explicitly limit the type of data and the categories of data subjects that can be subject to operational and strategic analysis. Once the data are filtered in line with the above Articles, then the retention period provided under Article 31 ER applies.

4.7. The EDPS therefore disputes Europol's assertion that the process of determining the DSC, whenever not achievable from the outset, is covered by and included within the objectives, tasks and competencies set out in the Europol Regulation. The inquiry has shown that, on the contrary, this operational need is new and arises from the fact that over the last years, Member States have increasingly been sending larger volumes of data to Europol. The nature of the data collected at national level in the context of criminal investigations and criminal intelligence operations is not limited anymore to targeted data but also includes the collection of large datasets. More digital content is generated and thus available for law enforcement in the context of criminal investigations, which, in turn, impacts the methods used to produce criminal intelligence.[25]

4.8. Thus, as established in the EDPS decision of 17 September 2020, the retention of datasets lacking a DSC for an undefined period and potentially throughout the duration of a criminal investigation, which can last ten years, is in breach of Article 18(5) and Annex II.B ER. This practice, especially in relation to large datasets, generates a high risk that Europol processes data of persons who do not fall under any of the categories of data subjects listed in Annex II.B of the Europol Regulation for long periods of time, i.e. for three years, renewable, if deemed necessary and proportionate in the context of the ongoing criminal investigation.

4.9. To prevent such a risk, the legislator included strict safeguards in the Europol Regulation. Namely, by including Annex II.B ER, the legislator introduced a requirement that data shared with Europol should only concern individuals who have a clearly established link with criminal activity, i.e. that they are considered by national law enforcement authorities as 'suspects', 'potential future criminals', 'witnesses', 'victims', 'contacts', ''associates' or 'informants'. Such a restriction can be understood when considering the risk stemming from the transmission of personal data from the level of national police to Europol, where data will be shared with other law enforcement authorities and cross-checked with information coming from other countries. Such further processing significantly magnifies the potential impact and risks for the data subject already existing at national level.

[25] 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), §3.9.

4.10. The EDPS acknowledges the operational considerations put forward by Europol regarding the volume of seized material in the field of digital forensics and intercepted communications, as well as the need to analyse datasets in detail before assigning a DSC.[26] Faced with this new situation, the EDPS understands that Europol needs, for technical reasons, some time to process these large datasets for the sole purpose of extracting relevant information.

4.11. However, the processing of datasets of persons not having undergone the categorisation should be limited to the shortest time necessary to materially proceed to such categorisation, where the originating Member State was not able to do so prior to the sending of the contribution because of the volume, size or format of the contribution. This is important to ensure that the processing of data of persons, whose link to the crimes for which the operational analysis is performed has not been established within the meaning of Annex II B ER, ceases as soon as possible.

4.12. Article 28(1)(e) ER provides in that sense that personal data is not kept longer than necessary for the purposes for which it was processed.

4.13. In order to define the maximum data retention period, it is necessary to refer to the purpose of the processing, which, in this case, is to ensure compliance with Article 18(3) and (5) read in light of Article 28(1)(c) ER. Such a maximum data retention period cannot therefore be linked to the duration of the criminal investigation to which they relate, contrary to other datasets whose processing conform to the provisions of the Europol Regulation. The retention periods defined under Article 31 ER are meant to apply to datasets the processing of which complies with the provisions of the Europol Regulation, i.e. datasets that have been lawfully shared with Europol and comply both with Article 4 and Article 18 ER, including the restrictions contained in Article 18(5) ER. These datasets have undergone a series of filtering operations to ensure their compliance with the data minimisation principle, i.e. with the guarantee that these data are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4.14. The EDPS notes that Article 18(6) of the Europol Regulation provides for a maximum period of six months for Europol to temporarily process data for the purpose of determining whether such data are relevant to its tasks and, if so, for which of the purposes referred to in Article 18(2) (cross checking, strategic or operational analysis, facilitating exchange of information between Member States, Europol, Union bodies, third countries and international organisations).

4.15. However, the Europol Regulation does not provide for a situation where Europol would be authorised to temporarily process personal data not falling in the categories of data subjects foreseen in Annex II.B ER for the sole purpose of verifying if personal data received fall into those categories and extracting relevant data for operational analysis.

4.16. Nor does the Europol Regulation contain specific provisions concerning the retention period of personal data that are relevant to Europol's tasks in accordance with Article 18(6) but for which there is no certainty as to whether their processing is compliant with other fundamental requirements for processing of the Europol Regulation.

[26] Europol letter of 20 October 2021, EDOC#1191646v7B.

4.17. In the light of the above, Article 18(6) ER provides the closest proxy to the practice of processing datasets for the purpose of extracting data that is in compliance with Annex II.B ER.

4.18. In the absence of an explicit legal provision laying down the retention period of personal data processed for this purpose, the EDPS considers it appropriate to make an interpretation by analogy of Article 18(6) ER. This article regulates the case where there is no certainty that the data received are relevant for Europol's tasks and thus in compliance with the ER, a situation which is comparable to the one at stake: the data received are relevant for Europol's tasks in line with Article 4 ER and have been accepted under Articles 18(2)(b) and (c) and Article 18(3) ER, i.e. for operational or strategic analysis purposes, but there is no certainty that they comply with the rest of the requirements of the Europol Regulation, in particular with Article 18(5) and Annex II.B ER.

4.19. Applying by analogy the maximum time-limit foreseen in Article 18(6) would allow for an initial processing of data in a pre-analysis phase, that appears appropriate to deal with large datasets, while imposing the maximum time limitation necessary to allow for this task to be fulfilled in compliance with the data minimisation and the storage limitation principles.

4.20. The EDPS considers that a six months retention period should apply to all datasets processed without a DSC by Europol, irrespective of the context of their collection. The Europol Regulation in force makes no distinction between data collected in the context of ongoing, specific, criminal investigations (including Joint Investigation Teams and Operational Task Forces) and other personal data processed for operational analysis. It is thus not possible to apply a specific regime to these datasets.

4.21. Furthermore, such an initial 'pre-analysis' processing, subject to a six months retention period, should take place prior to, and be entirely separate from, Europol's processing for purposes of strategic analysis, operational analysis or exchange of information, as would be ensured by the application of the set of mitigation measures by Europol under its Action Plan of 17 November 2020.

4.22. In light of the above, the EDPS finds that:

- By providing for the continuous storage of datasets lacking a DSC, the Action Plan provided by Europol does not address the infringement identified in the admonishment decision of 17 September 2020. Europol's continued processing of personal data of individuals, beyond the restrictive list provided in Annex II.B of the Europol Regulation represents a serious interference with the fundamental right to data protection of the persons concerned. Nor does the enhanced review process, foreseen under the Action Plan, prevent the continuous storage of this data for prolonged time periods with no set deadline.

- The processing by Europol of datasets lacking a DSC, as defined in Section 4 of this decision, for the sole purpose of extracting relevant information in compliance with Articles 18(3), (5), and Annex II.B ER, as well as the principles of data minimisation and storage limitation (Article 28(1)(c) and (e) ER), cannot exceed a maximum period of six months as from the date of reception of the contribution.

5. Corrective measures

5.1. In his Decision of 17 September 2020, the EDPS considered that it was not appropriate to impose an order of erasure of personal data pursuant to Article 43(3)(e) ER, despite the severe impact of such personal data processing activities on data subjects' fundamental rights and freedoms. Instead, the EDPS urged Europol to implement all necessary and appropriate measures to mitigate these risks.

5.2. Despite requests from the EDPS, Europol continues to refuse to define a maximum data retention period for the processing of datasets lacking a DSC, that would ensure that these datasets would not be retained for longer than necessary for ensuring compliance with Article 18(3), (5) and Annex II.B ER whenever the originating Member State would not have conducted the DSC because of the size and volume of the datasets.

5.3. As a consequence, large amounts of personal data about individuals for whom a link is not established with the criminal investigation within the meaning of Annex II.B ER are being processed by Europol on a continuous basis.

5.4. It thus appears necessary to remedy this breach of Article 18(3), (5) and Annex II.B ER by applying corrective powers on the basis of Article 43(3)(e) ER.

5.5. It is necessary to lay down the maximum retention period for datasets lacking data subject categorisation.

5.6. The EDPS understands that the datasets lacking data subject categorisation normally have not undergone the extraction process and therefore have not been shared with third parties. However, it is necessary to cater for the possibility that some datasets lacking data subject categorisation may nevertheless have been extracted and shared with third parties. Therefore, it is appropriate to order Europol to notify such third parties of their erasure, where appropriate.

5.7. The EDPS acknowledges that the process of identifying existing datasets lacking data subject categorisation and the clearing of the backlog might take some time given the amount of information processed by Europol. Therefore, an appropriate deadline should be set for the deletion of the existing non-compliant datasets, starting from the date of notification of the present decision.

5.8. In order to ensure proper monitoring of the implementation of the present decision, Europol should issue regular reports to the EDPS.

THE EDPS THEREFORE ORDERS AS FOLLOWS:

1. As from the day following the notification of the present decision, Europol shall, for each contribution, proceed to data subject categorisation within the meaning of Article 18(5) of the Europol Regulation within six months as from the date of reception of that contribution. Datasets lacking data subject categorisation at the expiry of the six months period referred in the previous sentence shall be erased.

2. By way of derogation from point 1 above, Europol shall proceed to data subject categorisation within the meaning of Article 18(5) of the Europol Regulation of all datasets existing on the day of notification of the present decision within twelve months from the day of said notification. Datasets lacking data subject categorisation at the expiry of the twelve months period referred in the previous sentence shall be erased.

3. Europol shall notify the erasure of the datasets to the third parties to whom datasets lacking data subject categorisation have been disclosed, where applicable.

4. Before the data subject categorisation within the meaning of Article 18(5) of the Europol Regulation is completed, no personal data in the contributions can undergo any form of processing by Europol other than that strictly necessary to proceed to such categorisation.

5. For a period of twelve months as from the day of notification of the present decision, Europol shall provide every three months reports on its implementation. Each report shall be divided in two sections, one related to point 1 above (data subject categorisation and/or deletion of contributions received as from the day following the notification of the present decision) and a second one related to point 2 above (data subject categorisation and/or deletion of existing datasets). Each section shall include at least the following information with regard to contributions:

a) references of the SIENA number of the contribution(s);
b) identification of the contributing entity;
c) date of receipt of the contribution and date of completion of the data subject categorisation and/or of erasure of the datasets;
d) notifications of erasure to third parties in application of point 3 above.

The section on point 2 of each report shall also include information on the progress achieved through quantitative indicators as to the data subject categorisation or erasure out of the total amount of existing data lacking data subject categorisation at the date of notification of the present decision.

6. Judicial remedy

6.1. Pursuant to Article 48 of the Europol Regulation, any action against a decision of the EDPS can be brought before the Court of Justice of the European Union within two months

from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.

Done in Brussels, 21 December 2021

(e-signed)

Wojciech Rafał WIEWIÓROWSKI