The Hague,	17 November 2020		
EDOC#	1131384	v	14A

Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge'

Contents

1. Background

The European Data Protection Supervisor (EDPS) Decision[1] on Europol's processing of large datasets (referred to as 'Europol's Big Data Challenge') was received on 18 September 2020. The EDPS concludes that the current practice of processing large datasets, for Europol to fulfil its mandate in responding to the operational demands of EU Member States (MS), results in a structural non-compliance risks with regard to the relevant provisions of the current Europol Regulation (ER). The EDPS decided that for the time being, mitigation measures under Article 43 (3) (b) (e) and (f) of the ER are not appropriate.

The EDPS Decision focusses on Europol's analysis tasks performed on the Computer Forensic Network (CFN) under Article 18 (2) (b) and (c) of the ER, emphasising that, in connection with Article 18(5) of the ER, Europol must not process personal data beyond the categories of data subjects (suspects, potential future criminals, contacts and associates, victims, witnesses and informants of criminal activities), as referred to in the Annex II of the ER for the purpose of analysis.

At the same time, the EDPS highlights that it is not possible for Europol, from the outset, upon receiving large datasets, to ascertain that all underlying information complies with the list of data subject categories.

The EDPS infers that this leads to Europol processing personal data for which it is uncertain that these comply with the corresponding categories of data subjects foreseen in the ER for the purpose of analysis. The EDPS also ascertains that this occurs over a longer period of time, thus

[1] European Data Protection Supervisor (EDPS) Decision, D(2020) 2036, C(2019) 0370, 18 September 2020 (releasable version published on www.edps.europa.eu)

requiring particular attention with respect to the principle of data minimisation (Article 28 (1) (c) of the ER).

From an overall perspective, the EDPS Decision implies that Europol's handling of information for its analysis work (and beyond that for all operational processing purposes based on Article 18 (5) in connection with Article 18 (2) of the ER), does not include, except for the possibilities provided for in Article 18 (6) of the ER to determine relevance for Europol's tasks, activities to identify and segregate relevant data (including from large datasets received), but has to commence on the basis of pre-sifted information containing only information of data subject categories of Annex II of the ER (i.e. suspects, potential future criminals, contacts, associates, victims, witnesses and informants of criminal activities).

The purpose of Europol's work and the very nature of analysis, according to Europol's current and previous legal frameworks, includes the process of minimising and aggregating information and data, by filtering and reducing the information contained in large datasets to what is relevant for operational support, as well as the related investigations, including to establish whether concrete criminal acts have been committed or may be committed in future.

Against this background, next to the information presented in this Action Plan, addressing the **EDPS Decision requires that the ER is modified with a view to clarifying and adjusting the competences of Europol pertaining to information processing activities in a manner which complies with EU data protection standards while preserving Europol's ability to provide MS' competent authorities with the operational support they require in the exercise of their duties also in future**.

Europol, therefore, calls for an amendment of its legal basis, in line with the operational requirements of EU MS. In light of the EDPS Decision, and in the context of current initiatives to strengthen the Europol mandate[2] and to identify key aspects for the future of Europol, as reflected in the **Council Resolution on the Future of Europol**[3] and the **Joint Statement by the EU Home Affairs Ministers on the recent terrorist attacks in Europe**[4] which calls for "… revising the Europol mandate with a strong legal basis for the handling of large datasets …", the European Commission is assessing the need to clarify the provisions on information processing activities by Europol, with a view to enabling the organisation to continue fulfilling its mandate effectively and in full compliance with fundamental rights.

The recast of the ER, which is initiated by the European Commission, provides a unique opportunity to address the structural legal concerns of the EDPS, in order to ensure that Europol will uphold its ability to comply with its mandate and provide operational support to EU MS in their fight against serious crime and terrorism. In light of the above elements, Europol sees an urgent requirement for maintaining a balanced approach between operational demands and data protection safeguards.

2. Europol's Action Plan

2.1. Context

The protection of personal data is a fundamental element of modern EU law enforcement work. Europol has a strong data protection regime and firmly stands behind the high standards established by the organisation, on the basis of the standards at EU level and in MS.

[2] European Commission Work Programme for 2020 (COM(2020) 37 final (29 January 2020))
[3] Council Resolution on the Future of Europol (Council Secretariat 12463/20 ENFOPOL 264)
[4] Joint Statement by the EU Home Affairs Ministers on the recent terrorist attacks in Europe, www.consilium.europa.eu

This document sets out an Action Plan detailing Europol's current and planned efforts to meet the EDPS's expectations regarding data processing in order to address the elements brought forward in the EDPS Decision.

The scope of the Action Plan is to help reduce the risks for data subjects by ensuring an enhanced data review, and to continue Europol's efforts for building a dedicated New Forensic Environment (NFE), which provides additional features and improvements to Europol's operational environment for handling large datasets on a new technical platform. Both aspects of the Action Plan relate to fundamental information security principles as well as to data protection controls which Europol is currently implementing.

2.2. Europol's current data landscape

Europol's role is to support and strengthen action by the competent authorities of MS in preventing and combating serious and international crime, including cyber-crime and terrorism, affecting two or more MS (Articles 3 and 4 of the ER).

The main support that Europol is delivering lies in analysing data provided by MS. The analysis of data can be performed in the format of operational, strategic or thematic analysis. Analysis always requires the setting of inferences and a hypothesis, as well as of recommendations for actions for the customer (MS) of the analysis, the national authorities.

The tasks of Europol are set out in Article 4 of the ER which states that Europol can collect, store, process, analyse and exchange information (data), including criminal intelligence.[5]

Europol also offers the possibility to MS to directly cross-check data. MS can directly search in Europol's Information System (EIS) for hits with their own datasets.

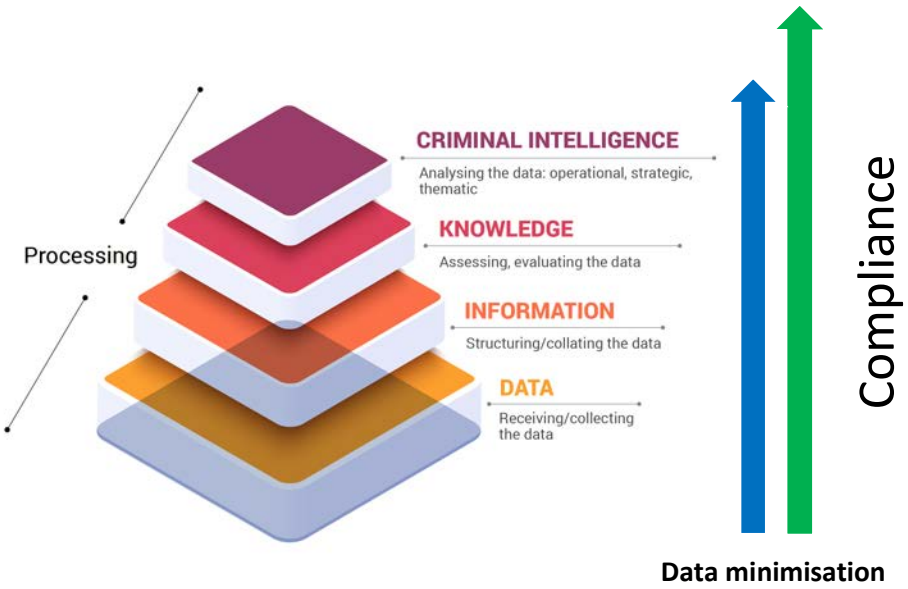
Both the analysis and the cross-checking are regulated in Article 18 (2) of the ER. Before analysis can be performed, there is an underlying process preceding the analysis activities.

The Action Plan presented below focusses on the process preceding the analysis work, as this is where the challenges with respect to the Data Subject Categorisation (DSC) in line with Annex II of the ER materialise, and which are responded to by the enhanced data review set out in this Action Plan. This is also the environment for which the NFE is being developed.

2.3. Enhanced data review

Performing the role as the EU Criminal Information Hub, Europol regards data protection as a strength and an essential component of the organisation's core business. An enhanced data review mechanism will be put into place, strengthening the data review arrangements currently in place. The objective of this mechanism is to detect at an early stage data files and contributions in which the DSC is not yet assessed or is in the process of being determined. The proposed actions will be implemented across the different relevant stages of Europol's data landscape. The aim of the actions is to enhance the data review and to increase the compliance along the process of data minimisation and data structuring before the analysis is performed.

[5] Article 2 (k) of the Europol Regulation defines processing broader than Article 4. Article 2 (k): collection, recording, organisation, structuring, storage, adaptation or alteration retrieval, consultation, use dissemination, alignment or combination, restriction, erasure, destruction.



2.3.1. Five actions to enhance Europol's data review activities

Taking into account the **scope of the EDPS Decision** on Europol's processing of large datasets (referred to as 'Europol's Big Data Challenge'), the following **five actions** are foreseen:

1) **Europol will explore the possibility to flag contributions for Europol in SIENA, concerning which the DSC is pending.**

- Activity: In the information exchange between MS, operational cooperation partners and Europol, those contributions concerning which the data is pending assessment or determination of the DSC shall be flagged by the contributor. Europol's Secure Information Exchange Network Application (SIENA) will be updated in order to realise this technical change which will be included as a priority in the ICT work planning for 2021. The SIENA user community will be consulted, and prior agreement with MS regarding their impact at national level will be obtained, including as per the regular arrangements for SIENA developments (e.g. via the Product Management Forum – PMF).

Europol will review and adjust the criteria to accept/reject incoming contributions, to prevent the inflow of data without DSC where required. All concerned staff members will be properly informed about the obligation to apply the updated criteria.

- Expected result: The envisaged labelling in SIENA will allow Europol to better assess the data received and to understand from the beginning the nature of the data collected. This will also allow to determine how users of this data will handle this data further and who will have access.

- Actionee: Europol, in close cooperation with Member States and operational cooperation partners.

2) **After accepting a request for support by MS or operational cooperation partners, Europol will label all relevant data files in its data environment for which the DSC assessment or determination is pending.**

- Activity: Those contributions accepted but still in the phase of assessment or determination of the DSC will be flagged in Europol's data environment. Europol's current analysis environment will be updated to ensure the implementation of this activity.

The resulting changes will be included in the ICT work planning for 2021 – however a manual flagging will start before the end of 2020.

Europol will also verify with the data providers if there is a need to store the original data in order to maintain the chain of evidence.

- Expected result: The flagging in Europol's data environment will represent a 'signpost' to those having access to this dataset that not all data already have a determined DSC. This will mitigate the risk that data without a DSC is further "processed", or integrated into the analysis work.

- Actionee: Europol

3) Implement additional measures by limiting access rights for data files where DSC is pending and enhancing data minimisation

- Activity: Europol will define, in consultation with the respective contributor of the information (MS and operational cooperation partners) and Europol's Data Protection Officer (DPO), the access rights for those files pending a determination of the DSC (in the current CFN).

Europol will limit the number of persons having access to data without an assigned DSC and the type of processing operations throughout the overall workflow:

- Raw data will only be processed by, and accessible to, a dedicated number of analysts/specialists.
- During the extraction, there is data minimisation, based on the restrictions in the respective Analysis Project (AP) opening decision (categories of data subjects, crime area, relevance and in agreement with the data provider (on what is expected/needed)).
- The extracted data will undergo another review by the analysts/specialists of the AP, in order to further reduce the amount of data and to ensure compliance.
- Once the data has been properly reviewed, the data will then become available and accessible to a large group of users, via the Unified Search Engine (USE) and/or the Europol Analysis System (EAS).

The technical implementation will follow the NFE Action Plan (see also Section 2.3.2. below).

- Expected result: The datasets will be only accessible by Europol staff who is involved in the process of determining the DSC, eliminating the risk of including a non-categorized entity in a Europol analysis product.

- Actionee: Europol

4) Every Analysis Project (AP) will be asked to increase the regular reviews of large datasets to check the alignment data with Annex II of the ER and the relevant data categories (defined in the AP Opening Decision).

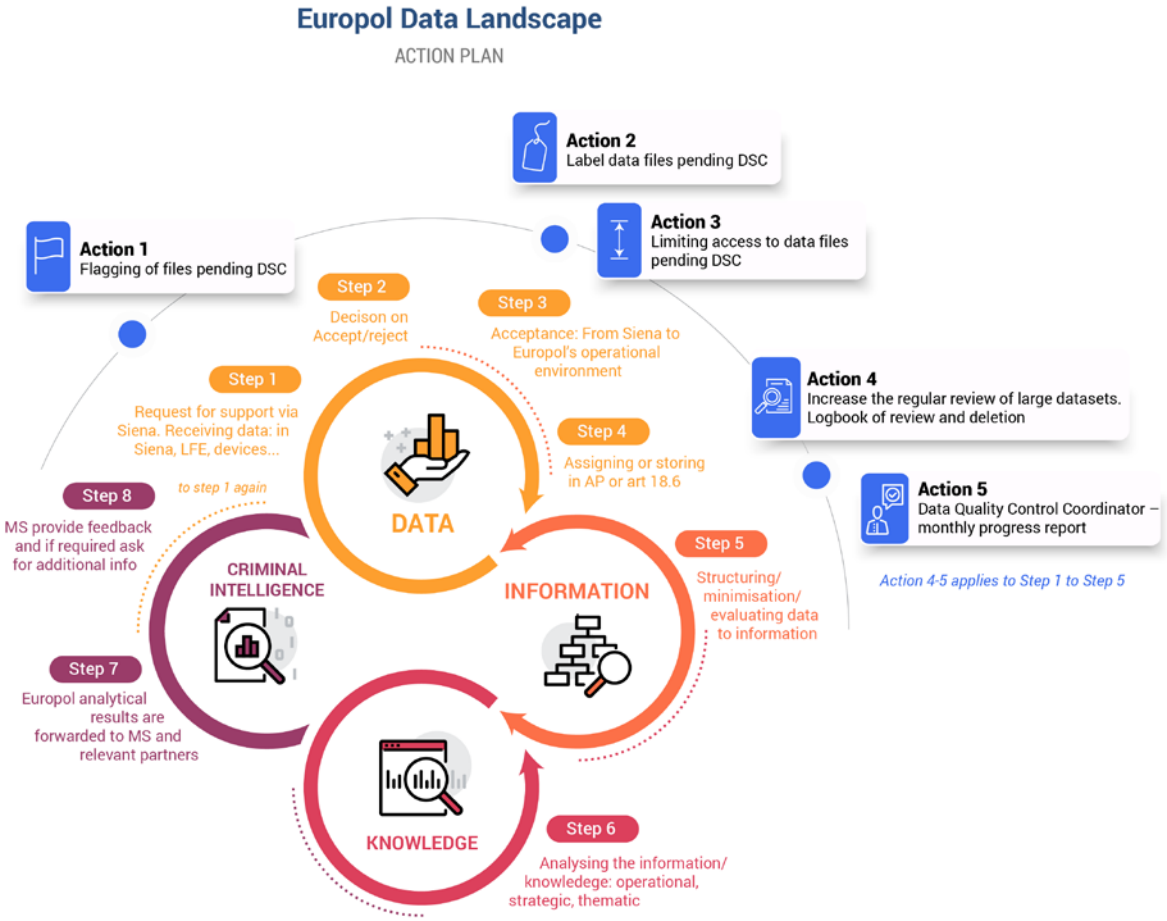
- Activity: Each AP will keep a logbook of review and actions taken. The recording of the deletion of information or files will be subject to the regular (audit) logging of activities in the respective system. This activity will start December 2020.

- Expected result: As the outcome of data review, file(s), which are not assigned with a DSC and are assessed as not necessary or proportionate, will be deleted in consultation

with the data owner, where this is feasible, in particular to preserve the chain of evidence and admissibility in subsequent judicial proceedings.

- Actionee: Europol, in consultation with the respective data owner (in Member States and concerning operational cooperation partners)

5) Europol appointed a full-time senior operational analyst as Data Quality Control Coordinator for the data review.



- Activity: In June 2020, a Data Quality Control Coordinator for Europol's Operations Directorate was appointed. The Data Quality Control Coordinator's work is to ensure the implementation of the current data review mechanism and that data processing is performed in line with the ER, in particular Annex II.

The Data Quality Control Coordinator will work in close cooperation with the DPO and produce a monthly progress reporting on the enhanced data review activities.

Europol will also establish a dedicated task force in the Operations Directorate (OD) to ensure the implementation of the activities outlined above.

The monthly progress reporting will pay particular attention to the labelling of specific files, the compliance with access rights, including the rejection and deletion of data. A summary of the progress reporting will be made available to EDPS on a quarterly basis.

- Expected result: The Data Quality Control Coordinator will help ensure the consistent implementation of the enhanced data review activities.

- Actionee: Europol

2.3.2. Design of the New Forensic Environment (NFE)

Europol initiated a project to establish a NFE at the end of 2019, replacing the current CFN. The NFE aims to provide a new forensic domain, for developing forensic activities in a secure and separate, dedicated environment. The new environment provides, among other features, enhanced access controls for limiting the impact for data subjects.

The proposed solution will facilitate different types of data processing in different purpose-specific domains.

The new forensic domain is designed to realise fundamental information security principles and practices (security by design, least privilege, need to know, defence in depth etc.) as well as a number of data protection controls (purpose limitation, data quality, data retention, data access rights, auditing), built-in by design and when applicable for the solutions concerned.

The data processed in this domain will be separate from the subsequent data processing for criminal analysis. As a result, any data or information originating from the forensic domain will be have a DSC assigned before it is processed in the analysis environment. The criminal analysis of data will take place in a different and specifically tailored domain (than the NFE).

The following specific security controls are being implemented:

- Europol's NFE will provide compartmentalised data areas with specific user profiles, isolating and limiting access.
- Identity and Access Management (IAM) that ensures governance of user lifecycle (provisioning, de-provisioning and entitlements management) will be implemented.
- Logging: The new NFE domain and any other solution introduced by the initiative will deliver robust audit logging provisions. Europol will keep records of the collection, alteration, access, disclosure, combination or erasure of personal data.

3. Conclusion

Europol is determined to make Europe a safer place. Processing and analysing data is at the core of Europol's support to MS. In past years, Europol's support has been instrumental to national law enforcement agencies, in particular in the areas of child sexual exploitation online, terrorism, cyber-crime and many forms of organised crime.

With this Action Plan, Europol aims to continue providing vital operational support to MS as well as operational cooperation partners, while ensuring that data protection is operated in line with the expectations of the EDPS.

In line with the outcome of the October 2020 MB meeting, Europol has informed the Chairperson of Management Board (MB) about this Action Plan. A dedicated discussion on the Action Plan will take place at the MB meeting in December 2020. In particular in view of the resource impact for Europol and MS with regard to the implementation of the Action Plan, guidance by the MB will be required on the way forward.

Subject to any further guidance from the MB and the EDPS, Europol will start the implementation of the actions under Section 2.3.1. from 20 November 2020 and will submit a first progress report to the EDPS by mid-March 2021. At the same time, Europol

will conduct an impact assessment of the new data review measures, in order to ensure that Europol upholds its capabilities to analyse and connect information about organised crime and terrorist activities across the EU.

The activities on the NFE will follow the project timelines and any variation will be communicated to EDPS.

Europol invites the EDPS to consider this Action Plan as a response to the Decision of 18 September 2020, covering the activities for which Europol can take action in cooperation with the relevant stakeholders.

Europol will inform the EDPS regularly about the status of the implementation of the planned data protection safeguards. This will allow Europol to receive valuable and timely feedback from the EDPS regarding its activities directed to address the admonishment decision. The guidance of the EDPS will further allow Europol, if necessary, to adjust measures at an early stage of development and implementation and to make therefore best use of the available resources.

Given that the implementation of the full scope of actions is dependent on MS and operational cooperation partners, as well as changes to Europol's systems, the achievement of the expected results will reach beyond the period of six months referred to in the EDPS Decision.

With respect to the elements of the EDPS Decision which require change to Europol's legal framework, it must be noted that this is subject to the recast of the ER, concerning which Europol is not involved as a formal actor in the legislative process. Further action from the EDPS with respect to the legal competence of Europol should therefore await the outcome of ER recast, with a view to ensuring that Europol can continue its core business activities.