EUROPEAN DATA PROTECTION SUPERVISOR

Case Reference
2021-0303

REPORT
ON
INSPECTION AT EUROPOL

pursuant to Articles
43(1) and (4) and 44(2) of Regulation (EU) 2016/794

20 December 2022

EDPS
Supervision & Enforcement Unit
and
Technology & Privacy Unit

This EDPS report is destined exclusively to the Services to which it has been expressly addressed and its content must not be communicated to other Services or third parties without the express written consent of the EDPS. Should this report inadvertently come into your possession and you are not a designated recipient, it should immediately be given to the Security Officer of your Service or to the Local Security Officer of the EDPS.

INSPECTION TEAM

[redacted]	Team leader, Head of Sector Area of Freedom, Security and Justice (legal)
[redacted]	Inspector (IT)
[redacted]	Inspector (IT)
[redacted]	Inspector (IT)
[redacted]	Inspector (legal)
[redacted]	Inspector (IT)
[redacted]	Inspector (legal)
[redacted]	Inspector (legal), expert from the German Supervisory Authority (Federal)
[redacted]	Inspector (legal), expert from the Dutch Supervisory Authority
[redacted]	Inspector (IT), expert from the Croatian Supervisory Authority

HEAD OF ACTIVITY / SECTOR

[redacted]	Head of Activity
[redacted]	Head of Sector Consultations and Audits

HEADS OF UNITS

ZERDICK Thomas	Supervision & Enforcement
VELASCO Luis	Technology & Privacy

SUPERVISOR

WIEWIÓROWSKI Wojciech Rafał	Supervisor

Contents

1. Executive summary

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of Regulation (EU) No 2018/1725 ('Regulation 2018/1725')[1] responsible for:

- Monitoring and ensuring the application of the provisions of Regulation 2018/1725 and any other EU act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by an EU institution or body;
- Advising EU institutions and bodies and data subjects on all matters concerning the processing of personal data.

Moreover, in accordance with Article 43 of Regulation (EU) No 2016/794[2] ('Europol Regulation' or abbreviated 'ER'), the EDPS is specifically in charge of monitoring the processing of operational data by Europol and ensure compliance with Regulation 2016/794 and any other Union act relating to the protection of natural persons with regard to the processing of personal data by Europol.

Regulation 2016/794 applies to Europol's processing of operational data and Regulation 2018/1725 applies to Europol's processing of administrative data[3].

To these ends, the EDPS fulfils the tasks and exercises powers provided for in Article 43 of Regulation 2016/794. Among his powers to investigate, the EDPS can conduct on-the-spot inspections. The power to inspect is one of the tools established to monitor and ensure compliance with Regulation 2016/794.

The formal decision was communicated to Europol by means of an Announcement Letter dated 19 July 2021. By a letter dated 31 August 2021, Europol was informed of a change in the dates of the inspection following a relevant request of Europol. The fieldwork was carried out on 27 and 28 September 2021 at the Europol premises in The Hague. The minutes of the inspection were sent to Europol for comments on 26 October 2021. EDPS received Europol's comments on 10 November 2021. The final minutes were sent to Europol on 17 December 2021.

This report summarises the findings identified during the inspection. Main findings and recommendations are included at the end of each section. A compiled list of all recommendations is inserted at the end of the report.

The recommendations contained in this report must be implemented in order to avoid possible breaches of Regulation 2016/794 within the deadlines provided in the respective section of the report. However, Europol is entitled within two months as of the reception of the report to suggest a different deadline for the implementation of the recommendations,

[1] 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 repealing Regulation (EC) No 45/201 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

[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.

[3] Article 46 of Regulation 2016/794 in conjunction with Article 99 of Regulation 2018/1725.

in case they consider that the provided deadlines cannot be met due to the efforts and investments required.

The EDPS will strive to take into account Europol's proposal to re-define the deadlines to be followed, at any rate, and will carry out a close follow-up of the recommendations.

In case the findings of this report indicate that there is a suspicion of breach of Regulation 2016/794, this will trigger the opening of a subsequent investigation or enquiry and it will be clearly stated in the report.

This inspection was part of the EDPS Annual Audit Plan for 2021.

2. Scope

Taking particular account of Europol's priorities and issues raised during 2021, the EDPS inspection focused on the development and use of artificial intelligence components for operational analysis at Europol and on the risk assessment process leading to the decision to submit a prior consultation to the EDPS under Article 39 ER.

The EDPS thus decided to target the following areas during the inspection:

1. The development and use of machine learning models for the analysis of operational data collected in the context of:

    a. the Joint Investigation Team (JIT) Operational Task Force (OTF) EMMA - which targets the now-defunct EncroChat communications platform;
    b. the Joint Investigation Team (JIT) OTF LIMIT - targeting a similar platform (Sky ECC);
    c. the Joint Investigation Team (JIT) OTF EMBARGO ;
    d. the OTF Trojan Shield / Greenlight - regarding the FBI-managed platform Anom and the compliance of the processing operations with Regulation 2016/794;

The technical team focused on checking compliance with the Europol Regulation of the development and testing process of machine learning models (in the context of OTF EMMA).

The legal team focused on checking compliance with the Europol Regulation of operational data processing activities within large-scale operational task forces.

2. The data protection risk assessment process in accordance with Article 39 ER.

3. Methodology

The inspection was performed in accordance with the procedures established in the **EDPS Audit Guidelines** (Adopted in November 2013, updated in October 2017 and November 2018) and the specificities of the follow up process with regard to Europol's inspections and by relying on the cooperation of staff members and managers of Europol to provide requested information, data, documents and access to premises.

In particular, **meetings and interviews** were set up and held with Europol staff to gather information and obtain access to relevant electronic databases, files and premises. Analysis, reviews and verifications of the information collected coupled with the outcome of physical examinations carried out by the EDPS team and **demonstrations** by Europol staff constitute the basis for the observations and recommendations in this report.

Minutes of the meetings were drafted in order to document the inspection procedures applied and provide for a transcript of the conversations with Europol staff. Two original copies of the minutes have been prepared, submitted for comments and signed by the team leader of the inspection team and by the Executive Director of Europol[4].

This **report** takes into account the documents provided by Europol before and during the on-site inspection (documents collected during the inspection are listed in **Annex 3**), as well as documents requested during the on-site inspection and provided afterwards (the latter being listed in **Annex 4**).

A list of **abbreviations** used in this report is included in **Annex 5**.

[4] For acknowledgement of receipt.

4. Analysis and recommendations - Compliance with Regulation 2016/794

4.1. Data protection risk assessment process

4.1.1. Background

The latest overall data protection reform aimed at ensuring consistent and high level personal data protection for processing operations carried out in the law enforcement context. In that context, a new Article 39 was introduced into the Europol Regulation. This Article provided for a new obligation to prior consult the EDPS in specifically defined cases, i.e. in cases where a new type of processing operation is to be carried out that either includes (a) the processing of special categories of data (as referred to in Article 30(2) ER) or (b) where the type of processing, in particular using new technologies, mechanisms or procedures, presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.

The previous obligation to consult the Joint Supervisory Body included in Article 10(2) of the 2009 Europol Decision[5] had different requirements and it was consistent with the Europol legal framework in place at that time, which focused on information systems and not on processing operations. Indeed, the Europol Management Board had to consult the Joint Supervisory Body only in case of establishing a new system processing personal data.

At the date of the inspection, the EDPS had received 11 prior consultation requests under Article 39 ER, issued an equal number of opinions and started to identify recurrent deficiencies in the process of the prior consultation, which were aggravated in the course of 2020 and 2021.

On 21 October 2020, the European Data Protection Supervisor ('EDPS') received from Europol a request for informal consultation[6] regarding:
(i) the appropriate legal basis for the development and use of Machine Learning ('ML') models in the context of a specific Joint Investigation Team ('JIT', i.e. a specific cross-border criminal investigation) and Europol's support to JIT countries and;
(ii) the need for a prior consultation under Article 39 of the Europol Regulation.

The EDPS considered that the processing of large amounts of personal data by using new technologies and in particular by developing and relying on ML models for identifying and prioritising decrypted communications represents a '*substantial change to the manner of processing*'[7], which was creating specific risks for fundamental rights and freedoms. It thus meets the conditions for prior consultation under Article 39 ER.

[5] Council Decision of 6 April 2009 establishing the European Police Office (Europol), OJ L 121, 15.5.2009, p. 37–66.

[6] Refer to EDOC #1132571 v3.

[7] The EDPS deferred the answer on the appropriate legal basis for a later stage as this would require further analysis.

Nevertheless, in January 2021, Europol shared with the EDPS, for information, a draft Data Protection Impact Assessment ('DPIA') with regard to the development and use of a 'Machine Learning toolbox' for operational analysis in the specific operation, which concluded that a prior consultation with the EDPS was not necessary. On 3 February 2021, the EDPS addressed a letter to Europol's DPO informing that he had decided to reclassify Europol's communication to a notification opening the Article 39 ER procedure.

On 10 February 2021, Europol submitted a formal notification under Article 39 ER[8], which included the final version of the DPIA, the identification of five specific risks for the rights and freedoms of the data subjects and their respective mitigation measures. However, the documentation was insufficient to allow the EDPS to assess compliance of the new processing operations with the provisions of the Europol Regulation. In particular, it did not include information on the selection of models to the use of operational data, including how all the processes were going to be monitored. Moreover, some of the risks identified were not specific to the development and use of ML models (e.g. unauthorised access to the data, processing of data that do not comply with the requirements stemming from Article 18(3), 18(5) and Annex II B ER), while other risks, such as risks related to the bias in the training and use of ML models or to statistical accuracy, were not considered. The EDPS decided to issue an opinion providing guidance to Europol with regard to the risks linked to the development and use of AI, which contained 21 recommendations[9].

The above illustrates some deficiencies in the data protection risk assessment conducted by Europol, which, in the first place, led them to consider that the development and use of ML models does not amount to a new type of processing operation presenting specific risks for the fundamental rights and freedoms, in particular the protection of personal data, of data subjects. Furthermore, the case reflects a broader tendency for Europol to provide the EDPS with prior consultation notifications under Article 39 ER, which include inaccurate or insufficient scoping/assessment of risks. The deficiencies observed were not specific to this case but are recurrent issues observed in several prior consultations. The need to extract relevant information from the different documents provided and to revert to Europol to obtain clarifications, also with regard to key risks not previously identified, results in prolonged delays in issuing opinions, or prevent the EDPS to make an assessment.

With the view of improving the prior consultation process on both sides and taking into account that a proper risk assessment by the controller is fundamental for the protection of the data subjects, the EDPS decided to inspect the data protection risk assessment process of Europol.

4.1.2. Criteria

The following **provisions and recitals of the Europol Regulation** are of particular relevance in this context:

- Article 28 (1) providing for the general data protection principles.
- Article 30 (2) with regard to the processing of special categories of personal data (i.e. of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life).
- Article 33 integrating in the Europol Regulation the principle of data protection by design (i.e. that Europol shall implement appropriate technical and organisational

[8] EDOC-#1148211-v2.

[9] EDPS Opinion of 5 March 2021.

measures and procedures in such a way that the data processing will comply with the ER and protect the rights of the data subject concerned).

- Article 38 providing that Europol is responsible for compliance with the principles referred to in points (a), (b), (c), (e) and (f) of Article 28(1).
- Article 39 providing for Europol's obligation to submit any new type of processing operation to the process of the prior consultation, where: (i) special categories of data as referred to in Article 30(2) are to be processed or (ii) the type of processing, in particular using new technologies, mechanisms or procedures, presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects. Moreover, Article 39 provides for the formal requirements of an admissible prior consultation notification as well as for the process before the EDPS.
- Article 41 (6) providing for the tasks of the Data Protection Officer ('DPO').
- Recital 40 according to which while the data protection rules of Europol are autonomous, they should at the same time be consistent with other relevant data protection instruments applicable in the area of police cooperation in the Union, as Directive (EU) 2016/680 ('LED')[10].
- Recital 50 underlining that the prior consultation mechanism serves as an important safeguard for new types of processing operations. The recital further clarifies that the prior consultation mechanism 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.

Although not directly applicable the following recitals of **Directive (EU) 2018/680 ('LED')** are of relevance when interpreting the notion of the 'risk':

- Recital 51 LED: The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analysing and predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
- Recital 52 LED according to which the likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing.

[10] 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, p. 89–131.

The EDPS also took into consideration the following **Europol internal documents**:

- [redacted]

[redacted]

Furthermore, the EDPS took into consideration the following **EDPS documents**:

- Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies (July 2019)[24].

4.1.3. Actions, findings and recommendations

[redacted]

[11] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]
[redacted]
[redacted]
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]	[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

4.2. Development and testing of machine learning models (in the context of Operational Task Force Emma)

4.2.1. Background

In the context of OTF Emma, Europol received a huge dataset of chat messages seized from a communication platform, concerning messages exchanged between criminals. The dataset includes approximately 65 million text messages and 350.000 images. Given the size of the dataset, Europol concluded that carrying out a manual analysis of the whole dataset would be highly inefficient and Europol does not have the human resources to take such approach.

In September 2020, Europol formed a team to assess how to process the OTF Emma dataset for operational analysis purposes. Europol's Data and AI Unit and Operations Unit jointly defined the tasks that ML models could perform on the OTF Emma dataset. In October 2020, the Europol's Data and AI Unit got access to the data and started the development and the definition of parameters of the models. The models are:

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

Europol's Data and AI Unit selected a set of pre-trained models that matched the functionalities defined. On the basis of the availability of training data, Europol decided to further train some of these models. Once the models were ready, their output would be accessible to the relevant analysts via a Chat Analysis Tool ('CAT').

As mentioned in section 4.1.1, on 21 October 2020, Europol consulted the EDPS about (1) the legal basis for the processing of operational personal data to develop and use the machine learning tools and (2) the necessity to conduct a prior consultation under Article 39 of the Europol Regulation (case 2020-0982).

Following the EDPS' answer to the second question, on 11 February 2021 Europol sent the EDPS a prior consultation request on the development and use of machine learning models for operational analysis (Case 2021-0130). Some days later Europol stopped the machine learning development process waiting for the EDPS answer to the consultation.

The EDPS considered that the processing of large amounts of personal data by using new technologies and in particular by developing and relying on ML models for identifying and prioritising decrypted communications represented a '*substantial change to the manner of processing*'[47], which was creating specific risks for fundamental rights and freedoms. It thus met the conditions for prior consultation under Article 39 ER.

Nevertheless, in January 2021, Europol shared with the EDPS, for information, a draft Data Protection Impact Assessment ('DPIA') with regard to the development and use of a 'Machine Learning toolbox' for operational analysis in the specific operation, which concluded that a prior consultation with the EDPS was not necessary. On 3 February 2021, the EDPS addressed a letter to Europol's DPO informing that he had decided to reclassify Europol's communication to a notification opening the Article 39 ER procedure.

On 10 February 2021, Europol submitted a formal notification under Article 39 ER[48], which included the final version of the DPIA, the identification of five specific risks for the rights and freedoms of the data subjects and their respective mitigation measures. Europol stopped the machine learning development process and waited for the EDPS answer to the prior consultation. However, the documentation was insufficient in order to allow the EDPS to assess compliance of the new processing operations with the provisions of the Europol Regulation. It did not for instance include information on the selection of models to the use of operational data, including how all the processes were going to be monitored. Moreover, some of the risks identified were not specific to the development and use of ML models (e.g. unauthorised access to the data, processing of data that do not comply with the requirements stemming from Article 18(3), 18(5) and Annex II B ER), while other risks, such as risks related to the bias in the training and use of ML models or to statistical accuracy, remained unidentified.

On 5 March 2021, the EDPS issued an Opinion providing guidance to Europol with regard to the risks linked to the development and use of AI, which contained 21 recommendations. These recommendations related to:

- Formal requirements of the DPIA;
- Necessity and proportionality;
- Data minimisation;
- Risks related to bias;
- Risks related to statistical accuracy;
- Risks related to errors;
- Risks related to security;
- Human intervention.

[47] See EDPS reply of 27 November 2020 to the informal consultation submitted by Europol (case file 2020-0982) and EDPS letter of 3 February 2021 (case file 2021-0130).

[48] EDOC-#1148211-v2.

The EDPS followed-up on Europol's implementation of these recommendations. By August 2021, Europol had addressed some of those recommendations while others regarding risk of bias, statistical accuracy and security were not fully implemented.

EDPS Inspection team focused on Europol's development of machine learning tools. Europol staff showed the inspection team the functioning of six of the seven ML models whose development stopped in February 2021.

Since the inspection, the EDPS has continued to follow-up Europol's implementation of the prior consultation recommendations by meeting Europol staff and analysing new and updated documents provided by Europol. However, actions taken by Europol after the inspection are formally out of its scope and will therefore be addressed in a separate document.

4.2.2. Criteria

The following **provisions of the Europol Regulation** are of particular relevance in this context:

- Article 28 (1) with regard to the processing according to the general data protection principles.
- Article 30 (2) with regard to the processing of special categories of personal data (i.e. of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life).
- Article 33 integrating in the Europol Regulation the principle of data protection by design (i.e. that Europol shall implement appropriate technical and organisational measures and procedures in such a way that the data processing will comply with the ER and protect the rights of the data subject concerned).
- Article 18(4) with regard to Europol's obligation of documenting its processing operations.
- Article 39(2) with regards to the obligation to assess the risks to the rights and freedoms of data subjects and the measures envisaged to address those risks.

Although not directly applicable, the following recitals of **Directive (EU) 2018/680 ('LED')** are of relevance when interpreting the notion of the 'risk'

- Recital 51 LED: The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analysing and predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in

order to create or use personal profiles; where personal data of vulnerable natural persons, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
- Recital 52 LED according to which the likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing.

The EDPS also took into consideration the following **Europol internal documents**:

- [redacted]

4.2.3. Actions, findings and recommendations

[redacted].

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

4.3 Operational data processing within large-scale operational task forces

4.3.1 Background

In light of the proposed processing by Europol of large datasets obtained in three of its recent Operational Taskforces ('OTFs'), Emma, Limit and Greenlight by means of several machine learning models, the EDPS inspection team verified whether Europol had already deployed any machine learning elements in the three inspected OTFs. The EDPS also checked compliance of the current processing practices within the three OTFs with the fundamental data protection principles enshrined in the Europol Regulation, in particular lawfulness, fairness[55], purpose limitation and accountability.

First, in order to implement the principle of purpose limitation, Europol should ensure that the scope of the personal data processed in the APs does not exceed the boundaries set out by Europol in the Analysis Project ('AP') Portfolio. Each AP hosted at Europol is created around a specific purpose, which is noted down at the start of each entry in the AP Portfolio, which can be specific commodity types, specific backgrounds of criminal organisations or a specific type of criminal investigation (the last one being the recently created AP on High-Risk Organised Crime Groups). The AP Portfolio itself implements Article 18(3) of the Europol Regulation, requiring Europol to define the specific purpose, categories of personal data and categories of data subjects, participants, duration of storage and conditions for access, transfer and use of the data concerned. In light of the volume and variety of the messages analysed within the OTFs, there is a risk that personal data are processed outside of the limits foreseen by these instruments.

Secondly, as the operations supported by Europol in the three examined OTFs are of an unprecedented scale and involve close cooperation with the investigation partners (both EU Member States and third countries), the EDPS inspection team looked into the existing tools and working arrangements that Europol relies on to ensure the lawful processing of personal data for these operations.

Third, as part of its obligations under Article 33 of the Europol Regulation on data protection by design, Europol is required to implement 'appropriate technical and organisational measures and procedures' to comply with the Europol Regulation and protect the rights of the data subjects concerned. Data protection by design is inextricably linked with the accountability of the controller, as described by the EDPS in its public accountability documentation[56]. The EDPS considers that the best way to ensure accountability, and to comply with the obligation of data protection by design, is to follow a structured approach to designing and documenting processing operations. As part of the accountability principle, Europol should ensure that the processes (including the tools that Europol relies on) are properly managed, documented and approved by the controllers so that the potential risks to data subjects are identified and treated at a sufficiently early stage, as not doing so both risks Europol overlooking potential critical harms to data subjects and risks non-compliance

[55] Notably how Europol ensures uniformity in the way it handles personal data across JITs, datasets and analysts.

[56] EDPS Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies Summary, v1.3, published on July 2019 on the EDPS website: https://edps.europa.eu/sites/default/files/publication/19-07-17_summary_accountability_guidelines_en.pdf.

with Article 33 of the Europol Regulation. The EDPS therefore requested and/or verified on-site, the relevant documentation for the tools deployed or used by Europol and its working arrangements with the partner authorities.

4.3.2. Criteria

The following **provisions of the Europol Regulation** are of particular relevance in this context:

- Article 5 containing the framework for Europol's participation to joint investigation teams.
- Article 17(3) laying out the possibility and the conditions for Europol to gain computerised access to national information systems.
- Article 18(2)(c), and 18(3) laying down the specific regime of purpose limitation at Europol with regards to its Operational Analysis activities in dedicated and specific Europol APs.
- Article 25 regarding the transfer of operational personal data to third countries.
- Article 33 integrating in the Europol Regulation the principle of data protection by design (i.e. that Europol shall implement appropriate technical and organisational measures and procedures in such a way that the data processing will comply with the ER and protect the rights of the data subject concerned).
- Article 40 ensuring that proper logging is performed for the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data integrity and security.

The EDPS also took into consideration the following **Europol internal documents**:

[redacted]

[redacted].

4.3.3. Actions, findings and recommendations

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]	[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]

[redacted]

5. Compiled list of recommendations and deadline for implementation

5.1. List of recommendations

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

5.2. Deadline for implementation

The EDPS will closely monitor the follow up of the above recommendations.

Europol should implement the above recommendations **within three months** as of the date of reception of this report, except for **recommendations** [redacted] which should be implemented within **six months**.

Annex 1 – Restricted information

Annex 2 – Powers of the EDPS

Article 43 of Regulation 2016/794 sets forth the powers of the EDPS as follows:

'...
3. The EDPS may pursuant to this Regulation:

(a) give advice to data subjects on the exercise of their rights;
(b) refer a matter to Europol in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;
(c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 36 and 37;
(d) warn or admonish Europol;
(e) order Europol to carry out the rectification, restriction, erasure or destruction of personal data which have been processed in breach of the provisions governing the processing of personal data and to notify such actions to third parties to whom such data have been disclosed;
(f) impose a temporary or definitive ban on processing operations by Europol which are in breach of the provisions governing the processing of personal data;
(g) refer a matter to Europol and, if necessary, to the European Parliament, the Council and the Commission;
(h) refer a matter to the Court of Justice of the European Union under the conditions provided for in the TFEU;
(i) intervene in actions brought before the Court of Justice of the European Union.
(j) order the controller or processor to bring processing operations into compliance with this Regulation, where appropriate, in a specified manner and within a specified period;
(k) order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation;
(l) impose an administrative fine in the case of non-compliance by Europol with one of the measures referred to in points (c), (e), (f), (j) and (k) of this paragraph, depending on the circumstances of each individual case'

4. The EDPS shall have the power to:

(a) obtain from Europol access to all personal data and to all information necessary for his or her enquiries;
(b) obtain access to any premises in which Europol carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.

...'.

Annex 3 – Documents collected during the inspection

[redacted]

Annex 4 - Documents requested during the on-site inspection and provided afterwards

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Annex 5 - List of abbreviations

AP	Analysis Project
CAT	Chat Analysis Tool
DPIA	Data Protection Impact Assessment
DPF	Data Protection Function unit
DPO	Data Protection Officer
EAS	Europol Analysis System
ECD	Europol Council Decision 2009/371/JHA of 6 April 2009 establishing Europol
EDOC	Europol Document
EDPS	European Data Protection Supervisor
HVT	High Value Targets
JIT	Joint Investigation Team
LED	Law Enforcement Directive (Directive (EU) 2016/680)
ML	Machine Learning
MS	Member State
OCG	Organised Crime Group
OTF	Operational Task Force
UAS	Unified Auditing Solution