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**:

- Article 39 ER EDPS prior consultation Process Description[11];
- Guidelines on the implementation of Article 39 Europol Regulation[12];
- Data Protection Impact Assessment (DPIA) template [13];
- DPIA on Machine learning toolbox for operational analysis in OTF Emma - Natural language processing and data extraction;[14]
- Draft commented DPIA on Machine learning toolbox for operational analysis in OTF Emma - Natural language processing and data extraction;[15]
- Notification to the EDPS regarding new type of processing operation 'Machine Learning Toolbox' (ARTICLE 39 ER) relevant to OTF Emma [16];
- Draft commented DPIA on the transfer of operational information to Europol with RSYNC and on the access to national environments to review content of data collected by national investigators[17];
- DPIA on Automated Entity Extraction [18];
- DPIA on OTF Limit [19];
- Draft commented DPIA on OTF Limit;[20]
- DPIA on OTF Greenlight [21];
- DPIA on Hidden Service De-anonymisation [22];
- DPIA on the Data Management Portal [23];
- Screenshots of the DPF Compliance Tool (general overview and specific entries).

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

The first inspection team (Team A) reviewed the risk assessment process leading to the decision to submit a prior consultation to the EDPS under Article 39 of the Europol Regulation. The team's fact-finding exercise focused both on the DPF and business owner's general understandings of the process (scoping, risk assessment methodology, follow-up procedures) and examined how the DPIA process was implemented in practical cases. The latter focused on the internal DPIAs prepared in the context of OTFs Emma, Limit and Greenlight (so-called 'Fast Development Projects') as well as the DPIA process in the context of long-running ICT projects including Quest+, and automated entity extraction.

[11] EDOC-#948171-v3.

[12] EDOC-#987546v7.

[13] EDOC -#901322-v11.

[14] EDOC # 1127278 v7.

[15] EDOC # 1127278 v1.

[16] EDOC-#1148211-v2.

[17] EDOC-#1102120 v 1.

[18] EDOC-#1071583-v1.

[19] EDOC-#1152667-v5.

[20] EDOC-#1152667-v1.

[21] EDOC-#1161832-v3.

[22] EDOC-#1035114-v4A.

[23] EDOC-#1180758-v1.

[24] https://edps.europa.eu/node/4582_en

To this end the first inspection team (Team A) met with the Head of Unit O1: Analysis and Strategic Coordination; the Head of Unit O2: EU Drugs; the Head of Unit and members O22: EU Organised Crime; the team leader of Unit O1-12: Information Hub; members of the Capabilities Directorate Business Product Management; the DPO and members of the DPF.

No DPF unit member was present during the interviews with Europol's operational staff in order to ensure independent responses by the latter. Instead, the DPF was interviewed separately on the subject matter i.e. on their involvement in the risk assessment process during a dedicated slot of 90 minutes.

All inspection activities are described in detail in the inspection minutes.[25] This section focuses on the most relevant inspection activities and in particular on activities, which triggered findings and recommendations.

a) *Scope of application of Article 39 ER*

The EDPS verified through the review of the relevant documentation and interviews with the Head of Unit O1; Head of Unit O2; Head of Unit and members O22; the team leader of Unit O1-12; members of the Capabilities Directorate Business Product Management; the DPO and members of the DPF, the existence and the implementation of a specific process with regard to the application of Article 39 of the Europol Regulation[26]. This process is further complemented by the Guidelines on the implementation of Article 39 Europol Regulation, which were updated in September 2021[27], and by a DPIA template[28].

The above documentation evidences the important contribution of the DPF to the correct application of Article 39 ER. Inspection findings indicate that the DPF has established close cooperation with the operational staff during the development of DPIAs and invests sizeable resources to providing guidance during this process.

[redacted]

Article 10(2) of the 2009 Europol Decision provided for the possibility for the Europol Management Board to decide on the establishment of a new system processing personal data. The Joint Supervisory Body had to be consulted and the Decision was subject to approval by the Council, which retained the final decision power. Article 10(3) specified that such decision should determine the conditions and limitations of this new system, in particular defining the purpose of the new system, access and use of the data, data retention periods and the categories of persons about whom data could be processed. Such systems could not in any case give way to the processing of sensitive data.

[redacted]

[25] Refer to inspection minutes, pp. 6-11 and 27-33.

[26] EDOC-#948171-v3.

[27] EDOC-#987546v7.

[28] EDOC -#901322-v11.

[redacted]

However, Article 39(1) ER does not refer to new systems but to ‘any new **type** of processing operation’.

Recital 50 ER specifies that ‘any new type of processing operation’ should not apply to specific individual operational activities, such as operational analysis projects (regulated under Article 18(3) ER), but to the use of new IT systems for the processing of personal data and any substantial changes thereto. However, Article 39(1)(b) ER, in offering indicatively examples of ‘type of processing’ that shall be subject to prior consultation, refers not only to the use of new technologies, but also to ‘mechanisms’ or ‘procedures’ presenting specific risks for the fundamental rights and freedoms of the data subjects.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[29] Refer to inspection minutes, p. 32.

[redacted]

[redacted] It could not be established either whether the transfer of operational information to Europol with RSYNC (name of the utility used for the synchronization of data with Europol) falls within this category as the RSYNC utility has already been used in past operational activities of Europol to handle the inflow of information (ex.: used by EU-IRU to support a live operation targeting jihadist communication channels)[31] but was nevertheless subject to a specific DPIA[32].

[redacted]

[redacted]

[redacted]

Findings

Finding 1	The DPF has established close cooperation with the operational staff during the development of DPIAs and invests sizeable resources to providing guidance during this process.
Finding 2	The DPF reads Article 39 and Recital 50 ER in the light of Article 10(2) of the 2009 Europol Decision, which limited prior consultations to new systems. This reading is not in line with the content of the internal Guidelines drafted by

[30] Refer to section 4.1.1. (Background of this report) as well as to EDOC # 1127278 v7.

[31] Refer to EDOC-#1102120 v 1.

[32] EDOC-#1102120 v 1

	the DPF and the wording of Article 39 ER, which refers to new types of processing.
Finding 3	[redacted]
Finding 4	It cannot be established whether the transfer of operational information to Europol with RSYNC (name of the utility used for the synchronization of data with Europol) falls within this category as the RSYNC utility has already been used in past operational activities of Europol to handle the inflow of information (ex.: used by EU-IRU to support a live operation targeting jihadist communication channels)[33] but was nevertheless subject to a DPIA.

Findings 3 and 4 provide indication that Europol may have breached Article 39 ER, for excluding the new types of processing activities listed under these findings from the scope of Article 39. As the breach is constituted only in case the new types of processing operations present specific risks for the fundamental rights and freedoms of the data subjects, the details of the processing operations for which there is an indication/suspicion that they were carried out in breach of Article 39 ER are presented in detail under the following sub-section b).

The EDPS has thus decided to open an investigation to ensure compliance with Article 39 ER.

Recommendations

In order to avoid the risk of non-compliance with the obligation to prior consult the EDPS under Article 39 ER, the EDPS also recommends that Europol:

Recommendation 1	*Clarify in the Guidelines on the implementation of Article 39 Europol Regulation the scope of application of Article 39. It should be clear that any 'new type of processing operations' refers to any use of new technology (including the use of new IT systems or substantial changes thereto), mechanisms or procedures, regardless of whether the 'new type of processing operation' is part of a well-known (established) process. The 'new type of processing operation' is subject to a prior consultation, in case it presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.*

[33] Refer to EDOC-#1102120 v 1.

Recommendation 2	*Raise awareness of Europol's operational staff on the scope of application of Article 39 ER by adding references to the amended Guidelines, to the process description and to the DPIA template. Europol should provide a detailed action plan as to how they intend to fulfil this recommendation within the deadline.*
Deadline:	*Three months after receipt of the report*

b) Risk assessment methodology (including threshold assessment)

The DPIA process aims to provide assurance that controllers adequately address risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply as well with the requirement of 'data protection by design' (Article 33 ER).

An integral part of any DPIA (following the description of the processing operations) is the risk assessment, which serves two purposes:

(i) Guiding the controller's decision on whether the threshold for a prior consultation with the EDPS is met (Article 39(1)(2) ER); and
(ii) Allowing data controllers to identify the risks the envisaged processing operations are posing to the data subjects' rights and to choose appropriate mitigation measures.
Hence, a solid risk assessment process and methodology is key for the correct implementation of Article 39 ER.

The EDPS[34] did not impose in his relevant guidance a standard methodology for carrying out DPIAs on EUIs. However, it was noted that any methodology used has to comply with the requirements of the applicable legal framework, i.e. in the case at hand with the Europol Regulation (Article 39). Although the EDPS has included in his guidance a template structure for a DPIA report, Europol has opted for using their own methodology and DPIA template, which does not by itself raise any issue as long as it caters for the purpose for which it is carried out.

[redacted]

The inspection activities have revealed that, as a result, the scoping of DPIAs is often too wide. For instance, the DPIA with regard to Operational Task Force ('OTF') Green Light[37] describes the reasoning for setting up the OTF, its investigative objectives and the tools used to allow Europol's direct access to the investigation data or for the transfer of data to Europol (which according to the DPIA did not constitute new types of processing operations as the

[34] Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies (July 2019). https://edps.europa.eu/node/4582_en

[35] As described in EDOC-#948171-v3 titled 'Article 39 ER EDPS prior consultation'.

[36] EDOC-#987546v7.

[37] EDOC-#1161832-v3.

tools were already used in OTF Emma and Limit). [redacted]

This issue is even more evident with regard to the so-called ‘internal DPIAs’. The EDPS identified via the inspection activities (and in particular via the interviews described in detail in the minutes) that in the context of the prior consultation process the DPF regularly requests completion of an ‘internal DPIA’ where the requirements of Article 39 ER are not met and therefore a full prior consultation procedure is not triggered.

The internal DPIA exercise appears to be used by default in cases of risky or sensitive processing and serves to act as a general compliance tool to promote awareness of data protection considerations among operational staff and business owners, and to allow the DPF to monitor the potential evolution of the processing operations concerned.

[redacted]

[redacted]

[redacted]

[38] EDOC-#1071583-v1.

[redacted]

Findings

Finding 5	Data controllers do not demonstrate a thorough understanding of the purpose of a DPIA, nor of the methodology for carrying out a risk assessment (identification of specific risks, and their impact on the data subject) as described in the Guidelines on the implementation of Article 39 Europol Regulation (part 7).
Finding 6	[redacted]
Finding 7	[redacted]

Finding 7 provides indication that Europol may have breached Article 39 ER, by not carrying out a proper risk assessment [redacted] that would allow Europol to identify possible specific risks to the rights and freedoms of individuals for the processing activities subject to this part of the inspection as well as appropriate mitigation measures with regard to the identified risks.

[redacted]

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

[39] EDOC-#1071583-v1.

[40] EDOC-#1102120 v 1.

[redacted]

The EDPS has thus decided to open an investigation to ensure compliance with Article 39 ER.

Recommendations

In order to avoid the risk of non-compliance with the obligation to prior consult the EDPS under Article 39 ER, the EDPS recommends that Europol:

Recommendation 3	*Amend part 7 of the Guidelines on the implementation of Article 39 Europol Regulation in order to clarify how the methodology for evaluating the risks for the fundamental rights and freedoms of the data subjects is linked to the assessment of whether the threshold for prior notification of Article 39 ER is met.*
Recommendation 4	*Clarify that part 7 of the Guidelines on the implementation of Article 39 Europol Regulation applies also in the 'internal DPIAs'.*
Recommendation 5	*Raise awareness among Europol's operational staff on the importance of the scoping of the DPIA and of the way to carry out a risk assessment (including the threshold assessment of whether the requirements of Article 39 ER to launch a prior consultation are met). Europol should provide a detailed action plan as to how they intend to fulfil this recommendation within the deadline.*
Deadline:	*Three months after receipt of the report*

c) *Demonstrating compliance with Article 39 ER*

Article 38(4) ER provides that Europol is responsible for compliance with the principles referred to in points (a), (b), (c), (e) and (f) of Article 28(1), i.e. with the fairness and lawfulness principle, the purpose limitation principle, the data minimisation principle, the storage limitation principle and the security of the processing. Read in the light of Recital 40 ER, according to which data protection rules of Europol, while autonomous, should be consistent with other relevant data protection instruments applicable in the area of police cooperation in the Union, as Directive (EU) 2016/680, Europol should also be able to demonstrate compliance with their responsibilities.

Proper documentation of the risk assessment carried out in the context of Article 39 ER (including the threshold assessment of whether the requirements for launching a prior consultation with the EDPS are met) is of key importance in order to:

(i) Allow Europol to demonstrate compliance with the Europol Regulation; and
(ii) Allow for meaningful supervision on the application of this provision.

The importance of the EDPS supervision on the application of Article 39 ER is also highlighted in recital 50 ER, which provides that the prior consultation mechanism is an important safeguard for new types of processing operations that allows the EDPS to monitor the lawfulness of the data processing carried out by Europol with complete independence.

Article 41(6) ER providing for the tasks of the DPO explicitly refers to the task of providing assurance that the Europol Regulation is internally applied with regard to the processing of personal data and to offering advice on data processing. Moreover, the Article 39 ER EDPS prior consultation Process Description[41] provides for a very distinct role of the DPF and the DPO in the context of this process.

The EDPS verified through the review of the relevant documentation and interviews with the Head of Unit O1; Head of Unit O2; Head of Unit and members O22; the team leader of Unit O1-12; the DPO and members of the DPF that (i) most of the steps of the prior consultation process[42] are properly documented and that (ii) Europol's DPF is closely involved from an early stage and offers ongoing guidance to the data controllers throughout the process.

However, the inspection activities revealed that the threshold assessment for submitting a prior consultation is not documented. The DPIA template[43] does not include a risk assessment table that would guide the data controllers in identifying the risks posed by the new data processing operation to the fundamental rights and freedoms of data subjects. This is only included in the Article 39 Notification to the EDPS and it is completed after the DPIA has been concluded and it has been decided that the specific processing operation shall undergo the prior consultation process.

However, the risk assessment should precede the decision on whether a specific processing operation should undergo the prior consultation process, as it is a prerequisite for the controller to be in a position to decide whether the Article 39 ER threshold is met.

This lack of proper documentation does not allow tracking the risk assessment that should have been carried out and thus the rationale behind decisions regarding the threshold assessment that triggers the application of the Article 39 procedure.

With regard to the 'internal DPIAs', the same level of documentation is not required as of the moment that it is decided that a full prior consultation procedure is not necessary. However, up to this point the same level of documentation is necessary to ensure that the risk assessment carried out and the decision on the application of the Article 39 ER procedure can be reviewed by the supervisory authority.

Furthermore, the inspection activities revealed that the advice of the DPF with regard to the scoping of the DPIA and the risk assessment process takes place primarily through informal meetings and exchanges, which are not documented[44]. Hence, there is no trace (in the form of meetings' minutes or emails) of the DPF's advice. The advice is fed into the (various iterations of) the draft DPIA, which is completed at the end, and as a formalisation, of this process. This makes it difficult to understand what DPF advice, if any, consisted of and why it was not followed, if that is the case.

[41] EDOC-#948171-v3.

[42] EDOC-#948171-v3 titled 'Article 39 ER EDPS prior consultation'.

[43] EDOC -#901322-v11.

[44] Refer to inspection minutes, pp. 6, 9, 32.

The impact of the lack of proper documentation on data subject rights is particularly serious, as there exists no means for the EDPS (as the supervisory authority) to review the risk assessment methodology applied and the proper justification of the decisions regarding the threshold assessment that triggers the application of the Article 39 ER procedure.

Findings

Finding 8	The threshold assessment for submitting a prior consultation is not documented.
Finding 9	The DPIA template does not include a risk assessment table that would guide the data controllers in identifying the risks posed by the new data processing operation to the fundamental rights and freedoms of data subjects. This is only included in the Article 39 Notification to the EDPS and it is completed after the DPIA has been concluded and it has been decided that the specific processing operation shall undergo the prior consultation process.
Finding 10	The advice of the DPF with regard to the scoping of the DPIA and the risk assessment process takes place primarily through informal meetings and exchanges, which are not documented.

Recommendations

In order to avoid the risk of non-compliance with the obligation to prior consult the EDPS under Article 39 ER, the EDPS recommends that Europol:

Recommendation 6	*Amend the Article 39 ER EDPS prior consultation process description in order to provide for proper documentation of:* *(i) The risk assessment, including the threshold assessment, that triggers (or not) the application of the prior consultation procedure (currently Article 39 ER). The recommendation also refers to 'internal DPIAs';* *(ii) The DPF's advice, in case it differs from the controller's decision on whether or not the criteria for mandatory prior consultation are fulfilled;*
Recommendation 7	*Reflect these amendments in the Guidelines on the implementation of Article 39 Europol Regulation and on the DPIA template by including a risk assessment table.*
Deadline:	*Three months after receipt of the report*

d) Demonstrating compliance with Article 39 ER in the context of 'fast development projects'

The EDPS identified through interviews with the Head of Unit O1; Head of Unit O2; the DPO and members of the DPF that the shortcomings identified above [45] are exacerbated in the context of 'fast development projects'. These are new kinds of projects faced by Europol where the Agency is obliged to react at short notice, responding to Member States' urgent requests for operational support, and apply new data processing tools in often sensitive political contexts (e.g. OTFs Emma, Limit and Greenlight).

In this context, the inspection activities revealed that there were cases where (contrary to the guidance offered in the Guidelines on the implementation of Article 39 Europol Regulation) the launch of the processing activities preceded the validation of the DPIA (e.g. the use of the RSYNC tool in OTF Emma). In conjunction with the lack of proper documentation (e.g. in the form of meetings' minutes or emails), the inspection team is not in a position to confirm whether the risk assessment process was indeed concluded before the launching of the processing operation.

The impact of carrying out the risk assessment process in very strict time frames is particularly serious on data subject rights as risks may remain unidentified. The importance of the correct interpretation of the scope of application of Article 39 ER and the correct scoping of DPIAs[46] (including a more targeted approach to risk assessment) becomes even more evident in the 'fast development projects' as it would allow the process to focus only on the new processing operations and on the specific risks deriving from these operations.

Findings

Finding 11	In the context of fast development projects, the launch of the processing activities preceded the validation of the DPIA.
Finding 12	In the absence of documentation of the risk assessment, it is not possible to verify whether the risk assessment process was indeed concluded before the launching of the processing operation.

Recommendations

In order to avoid the risk of non-compliance with the obligation to prior consult the EDPS under Article 39 ER in the context of fast-development projects, the EDPS recommends that Europol:

Recommendation 8	*Amend the Article 39 ER EDPS prior consultation process description in order to provide a mechanism to document, also in the context of 'fast development projects' (where the validation of the DPIA is not possible), and before the launch of the processing activities:*

[45] Under 4.3.1.(a), (b) and (c) of the present report.

[46] Refer to point 4.3.1.(a) and (b) of the present report.

	(i) the outcome of the threshold assessment (whether the Article 39 ER threshold is met or not - e.g. in the form of a note); and *(ii) in case the threshold is met, the risk assessment, which will be further detailed in the DPIA.*
Deadline:	*Three months after receipt of the report*

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:

- Facial Detection and Similarity Search: Detecting faces in the pictures and generating a numerical vector which is representative of the detected face that can be used to perform similarity search through all the pictures of the dataset.
- Image Similarity: generating a vector with information about each picture that analysts can use to find other pictures similar to a given picture.
- Image Classification: Detect certain classes of objects appearing in images, including documents for identification, QR codes, vehicles, bank notes, drugs, etc.
- Named Entity Recognition: Extract entities from text, such as person names, locations, company names, vehicle licence plates, etc.
- Machine Translation: translate text from other languages to English.
- Text Classification: Classify text messages to specific categories such as threat to life or money laundering.
- Robust Reading: Extract text from pictures, such as invoices, banknotes serial numbers, images of excel spreadsheets and others.

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**:

- EDOC-#1170152-v2-EMMA - Facial Detection and Similarity Search DP Assessment
- EDOC-#1169951-v2-EMMA - Machine Translation DP Assessment
- EDOC-#1169933-v2-EMMA - Image Similarity Search DP Assessment
- EDOC-#1169624-v2-EMMA - Text Classification DP Assessment
- EDOC-#1169515-v2-EMMA - Robust Reading DP Assessment
- EDOC-#1169494-v2-EMMA - Image Classification DP Assessment
- EDOC-#1169381-v3-EMMA - Named Entity Recognition DP Assessment
- EDOC-#1162317-v6-Policy on the Development and Use of Machine Learning Tools for the Purpose of Supporting Operational Analysis
- EDOC-#1160124-v6-Provide machine learning toolbox process (pr v 1)
- EDOC-#1184553-v3-Provide machine learning toolbox process description (20-09-2021)
- EDOC-#1182774-v1-LEAP - Software Development Methodology for Chat Analysis Tool
- EDOC-#1180599-v1-EMMA - Machine Translation Model Card
- EDOC-#1180598-v1-EMMA - Robust Reading Model Card
- EDOC-#1180596-v1-EMMA - Image Classification Model Card
- EDOC-#1179626-v1-EMMA - Facial Detection and Similarity Search Model Card
- EDOC-#1179621-v1-EMMA - Image Similarity Search Model Card
- EDOC-#1179611-v1-EMMA - Text Classification Model Card
- EDOC-#1179491-v1-EMMA - Named Entity Recognition Model Card
- EDOC-#1179854-v1-Data & AI - Security measures and controls limiting the access to the Machine Learning environment
- EDOC-#1179659-v1-Data & AI - Assessment and selection of machine learning techniques and pre-trained models
- EDOC-#1179637-v1-Data & AI - Procedure and tools to measure performance in machine learning models
- EDOC-#1175908-v1-Data & AI - Bias in AI
- EDOC-#1159717-v3-Chat_Analysis_Tool_-_Functional_requirements
- EDOC-#1163851-v1-CAT_Backlog
- EDOC-#1124467-v1B-NLP_training_of_production_system
- ML prototype
- Image Classification Classes

4.2.3. <u>Actions, findings and recommendations</u>

During the on-site activities, the inspection team met with the Head of the Data and AI Team, a senior specialist on ML, the Head of C13-LP. A DPF unit member was present during the interviews with Europol's operational staff. The interviews were followed by hands-on demonstrations of the ML models.

All inspection activities are described in detail in the inspection minutes.[49] This section focuses on the most relevant inspection activities and in particular on activities triggering findings and recommendations.

a) Missing ML model performance metrics and requirements

This is the first time Europol aimed at processing personal data using ML models. Data representativeness, i.e. how similar are the training, testing and validation datasets to the dataset the model will process once deployed, is a predictor of the model's performance.[50] Measuring the similarity between the OTF Emma dataset and the datasets used to develop the pre-trained models would allow Europol to ensure the training data of the models were representative enough. However, Europol could not know the characteristics of the OTF Emma dataset (e.g. Europol could not know the ethnic origin or gender of the data subjects appearing in OTF Emma images). Consequently, team B checked how Europol could ensure its compliance with the data accuracy principle in such a challenging scenario.

During the inspection, inspection team B asked the Data and AI Unit about the requirements for the chat Analysis Tool ('CAT') and the ML models and requested a copy of the documents defining the ML models' performance metrics and requirements.

The inspection team found that the Operations unit, which was the business unit who would use the CAT and the ML models, did not provide the Data and AI Unit with explicit performance requirements. Europol's documents describe only functional requirements (e.g. the classes of images to detect which is the minimum performance required to consider a model as ready for deployment).

The inspection team also found that while he document 'ML prototype' document' includes the 'Business requirements for chat visualisation tool including ML-based functionality', the requirements related to its ML models describe their functionality (e.g. search function for face similarity or extraction of text from pictures) not their expected performance.

The Data and AI Unit met regularly the Operations Unit to gather qualitative feedback. No record was made of these meetings. In addition to that, no evidence has been found that such qualitative feedback involved the models' performance or readiness.[51]

In the absence of properly defined performance metrics and requirements, Europol would have to rely on the subjective perception of its analyst on each model's performance when deciding if the models' outputs were accurate enough to be used for investigation activities.

[49] See inspection minutes, pp. 11-21.

[50] 'In a broad range of fields it may be desirable to reuse a supervised classification algorithm and apply it to a new data set. However, generalization of such an algorithm and thus achieving a similar classification performance is only possible when the training data used to build the algorithm is similar to new unseen data one wishes to apply it to. It is often unknown in advance how an algorithm will perform on new unseen data, being a crucial reason for not deploying an algorithm at all.' Schat E, van de Schoot R, Kouw WM, Veen D, Mendrik AM. The data representativeness criterion: Predicting the performance of supervised classification based on data set similarity. PLoS One. 2020 Aug 11;15(8):e0237009. doi: 10.1371/journal.pone.0237009. PMID: 32780738; PMCID: PMC7418972.
'Data representativity is crucial when drawing inference from data through machine learning models.' Clemmensen, Line Harder and Rune D. Kjærsgaard. "Data Representativity for Machine Learning and AI Systems." *ArXiv* abs/2203.04706 (2022): n. pag.

[51] How close a model is from reaching a performance level that would allow its deployment.

The EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[52] consider a set of key design and default accuracy elements. Among them stands the one requesting the processing of personal data to be 'measurably accurate'. Without formal and measurable performance metrics, it is not possible to have a measurably accurate processing.

The guidelines also state that data protection by design shall be implemented 'when the controller is deciding how the processing will be conducted and the manner in which the processing will occur and the mechanisms which will be used to conduct such processing [...] This includes the time of procuring and implementing data processing software, hardware, and services...'. [53]

Findings

Finding 13	In the absence of performance metrics it is not possible for Europol to ensure the output of the ML models will have a minimum quality or even what should be such minimum quality.

Finding 13 provides indication that Europol may have breached Article 28(1)(d) ER, which requires the processing of personal data to be accurate.

Finding 13 also provides indication that Europol may have breached the data protection by design requirement set in Art. 33 of the ER. The ML development process did not take into account the necessity to establish performance requirements and to select the measurements that would ensure if the models had achieved the required performance level.

The impact of the lack of performance metrics creates the risk of deploying a model that would produce erroneous outputs without additional safeguards. For example, an error in a model used to extract text from pictures could produce a wrong bank account number from an invoice. That could result in Europol investigating the links of an individual with a certain criminal activity when that individual is totally unrelated.

ML errors could be mitigated by human review. However, a lack of performance requirements increases the risk of the number of errors being so high that it might not be possible to manage them efficiently.

Recommendations

In order to avoid the risk of non-compliance with the obligations set under Articles 28(1)(d) and 33 ER in the context of the machine learning tool development and use, the EDPS recommends that Europol:

Recommendation 9:	*Define the performance metrics that will measure the performance of each of the ML models.*

[52] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted on 20 October 2020, par. 79.

[53] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted on 20 October 2020, par. 35.

Recommendation 10:	*Set required minimum value(s) for performance metrics so that ML models can be considered as reliable enough to be deployed in production.*
Deadline:	*Three months after receipt of the report*

b) Missing documentation on the processing operations

According to Art. 18(4) of the Europol Regulation, Europol can process personal data 'in compliance with the data protection safeguards provided for in this Regulation. Europol shall duly document those processing operations.' The same provision allows the EDPS to request those documents with the purpose 'of verifying the lawfulness of the processing operations.' Moreover, Article 28 provides that Europol should apply the general data protection principles (lawfulness and fairness; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality) to all its processing operations.

During the prior consultation and before the inspection, Europol provided three relevant documents: the process description for providing a machine learning toolbox (EDOC-#1160124-v6), the policy on the development and use of machine learning for the processing of operational data (EDOC-#1162317-v6) and a data protection assessment for each of the ML models (EDOC-#1170152-v2, EDOC-#1169951-v2, EDOC-#1169933-v2, EDOC-#1169624-v2, EDOC-#1169515-v2, EDOC-#1169494-v2 and EDOC-#1169381-v3). The inspection team collected updated versions of some of those documents during the inspection.

However, Europol did not draft any of these documents before or during the development of the ML models. Europol produced the documents after stopping the development and after the EDPS adopted its Opinion of 5 March 2021 with regard to the prior consultation (EDPS Case 2021-0130). As a consequence, the documents do not fully reflect what was done during the machine learning development period (for example, bias was not checked during the development) but they do reflect how Europol will process operational data in this context from the moment they were drafted.

On the question of how Europol will decide that a ML solution could be a suitable solution for a certain task, the Data and AI Unit staff explained that on the basis of their expertise they can advise the business units on what is possible or not. On that specific area, Europol stated that there was no formal procedure in place to perform and document such assessment, nevertheless there would be one in the future.

Europol's data protection assessments[54] document the process 'Providing machine learning toolbox' for each of the seven tasks where Europol was developing a ML model. Although the process includes a step to assess and mitigate the risk of bias, these data protection assessments do not constitute a data protection impact assessment as they do not identify the full spectrum of risks to which the models are subject nor the mitigation measures that Europol would apply.

[54] See EDOC-#1170152-v2-EMMA - Facial Detection and Similarity Search DP Assessment, EDOC-#1169951-v2-EMMA - Machine Translation DP Assessment, EDOC-#1169933-v2-EMMA - Image Similarity Search DP Assessment, EDOC-#1169624-v2-EMMA - Text Classification DP Assessment, EDOC-#1169515-v2-EMMA - Robust Reading DP Assessment, EDOC-#1169494-v2-EMMA - Image Classification DP Assessment and EDOC-#1169381-v3-EMMA - Named Entity Recognition DP Assessment.

Europol plans to mitigate the risks of errors and potentially biased models using human oversight. Indeed, one of the requirements of the Chat Analysis as documented in EDOC-#1163851-v1-CAT_Backlog is to 'Provide feedback for machine learning models (image types, entity types, text types)'. Europol staff explained the CAT would provide its users (operations unit analysts) a functionality to report errors. Afterwards, the Data and AI unit would use those error reports, whenever possible, to improve the model's performance or mitigate detected biases.

Findings

Finding 14	*Europol is missing a formal and documented procedure to asses if and under which conditions a ML model could be a suitable solution for a certain business requirements.*
Finding 15	*Europol did not perform a data protection impact assessment including a complete assessment of the risks to the rights and freedoms of data subjects when processing personal data using ML models and the CAT.*

Finding 14 provides indication that Europol may have breached Article 18(4) in conjunction with Article 28 ER with regard to Europol's obligation to document its processing operations and to apply the general data protection principles upon them. The lack of a formal and documented procedure to assess if and under which conditions a ML model could be a suitable solution for a certain business requirements increases the risk for data subjects because undocumented and informal processes cannot guarantee that Europol is consistently safeguarding the principles set out in Article 28 ER.

Finding 15 provides an indication that Europol may have breached Article 39(2) ER to the extent that the prior consultation request to the EDPS did not include the assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address those risks. Without a formal and holistic assessment of the risks posed by the use of ML models and the CAT to process operational personal data the risk of lacking appropriate safeguards for the rights of the data subjects is increased.

Recommendations

In order to avoid the risk of non-compliance with the obligations set under Articles 18(4), 28 and 39(2) ER in the context of the machine learning tool development and use, the EDPS recommends that Europol:

Recommendation 11:	*Draft a procedure describing how to assess the suitability of ML techniques with the available datasets for a given task defined by a business requirement.*
Recommendation 12	*Perform a data protection impact assessment for the ML models and the Chat Analysis Tool.*
Deadline:	*Three months after the receipt of the report.*

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**:

- The specific JIT agreements for the OTFs under inspection[57];
- The AP Portfolio;
- The DPIA on OTF Limit [58];
- Draft commented DPIA on the transfer of operational information to Europol with RSYNC and on the access to national environments to review content of data collected by national investigators[59];
- DPIA on OTF Greenlight [60].

4.3.3. Actions, findings and recommendations

During the on-site activities, the third inspection team (team C) met with the Heads of Unit of O22 and O1-12, the head of the Data & AI team, as well as members of O1-24, C14, O2 and EC3. A member of the DPF attended the interviews, which were followed by hands-on demonstrations.

All inspection activities are described in detail in the inspection minutes.[61] This section focuses on the most relevant inspection activities and in particular on activities which triggered findings and recommendations

[57] See Annex 1 (EU-restricted).

[58] EDOC-#1152667-v5.

[59] EDOC-#1102120 v 1.

[60] EDOC-#1161832-v3.

[61] See inspection minutes, pp. 22-26 and 38-42.

With regard to the first focal point of team C, the inspection team found that no novel machine learning functionalities were, at the time of the inspection, deployed by Europol with regard to the large datasets processed within the examined OTFs. Instead, operational analysts manually explore data they receive for relevant information to the investigation.

However, team C did find that the lack of certain analysis tools at Europol, in particular for visualisation of data, has prompted Europol to provide some of its analysts with real time access to national ICT environments (offered both by Member States and Third Countries[62]) that make chat application data available in a format that is easier to review for analysts[63].

a) Use of external platforms by Europol during the Operational Analysis process

The use of national ICT environments by analysts to access and explore chat messages appears to be a novel way of working at Europol. Although Europol, in its DPIA for OTF Limit[64], states that the 'functionalities implemented in these systems are neither considered as a new type of processing, nor as a substantial changes of existing ones', it does appear that the real time access to national environments itself is considered a new type of processing by Europol, prompting it to perform a DPIA.

The EDPS notes that for all three OTFs, Europol uses a Member State[65] interface to visualise information hosted at the national level, which allows analysts to replicate the user experience of a chat application and to display images, which Europol's own visualisation tool[66] does not allow. Variants of the same software were used for the different OTFs. The Member State interface has a download feature integrated, which Europol used only for specific content under review, meaning that no batch downloads were performed.

For OTF Greenlight, next to this Member State solution, Europol was provided with direct access to data a platform hosting similar operational data in a Third Country environment[67].

Process documentation

This type of processing of operational personal data using external tools does not appear in any process description provided to the EDPS at the time of the inspection. While a reference to the interfaces is included in the respective DPIAs conducted for OTF Limit and Greenlight, they do not appear to have been transposed into the general process descriptions used by Europol. This means that a process description is missing or that the provided process descriptions are missing steps related to the use of these types of interfaces.

For instance, while the EAS manual (chapter 8) foresees the possibility to transfer data to Member States, it does not further specify that Europol can make use of MS tools for processing operational personal data.

[62] See Annex 1 (EU-restricted).

[63] See EDOC#1152667v2, p.4.

[64] See EDOC#1152667v2, p. 3-4.

[65] See Annex 1 (EU-restricted).

[66] See inspection minutes, p. 39.

[67] See Annex 1 (EU-restricted).

The obligation to comply with data protection by design under Article 33 of ER should be interpreted[68] as requiring that process and procedure be fully documented as to ensure that, at each step of the process, data protection be taken into account. Without a clear process description, one cannot analyse each step of the process through the data protection lens and thus have assurance that data protection by design has been implemented correctly - i.e. a clear process description is one of the fundamental key aspect of data protection by design.

Lack of assurance of compliance with Article 17(3) ER

Article 17(3) ER provides a specific legal basis for Europol to access national, Union or international information systems and retrieve personal data stored therein.

This article states that where stricter rules governing access and use apply to the national information system, compared to the Europol Regulation, these stricter rules need to be followed by Europol. Where Europol accesses the national information system, it should therefore inquire as to any stricter rules it needs to consider and document the outcome.

[redacted]

Flagging

[redacted]

Logging

Article 40 ER provides for the obligation for Europol to keep records (in the form of logs or documentation) of any processing of personal data for the purposes of verifying the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security. Logs or documentation shall be communicated upon request to the EDPS, to the DPO or to the national unit concerned if required for a specific investigation.

[redacted]

[68] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020

[redacted]

[redacted]

[redacted]

Findings

Finding 15	This type of processing of operational personal data using national information systems does not appear in any process description.
Finding 16	[redacted]
Finding 17	[redacted]
Finding 18	[redacted]
Finding 19	Europol's use of the national environments is not limited to pure retrieval, but also allows Europol to convey some information to the other (national) officers working on the dataset - for instance by tagging already analysed data, which would mean that Europol is interested in the data it tagged. It is however unclear how much information is made available to the third country through the flagging and thus to what extent this would qualify as a transfer from Europol to the recipient.

Finding 16 indicates that Europol should demonstrate compliance with Article 17(3) ER.

Finding 17 indicates that Europol has breached Article 40 ER, as without adequate logging, [redacted]

Given findings 16, 17 and 19, the EDPS has decided to open an enquiry to obtain additional information about the use of national information systems by Europol.

Recommendations

In order to avoid the risk of non-compliance with the obligations stemming from Articles 17(3), 33 and 25 ER, the EDPS recommends that Europol:

Recommendation 13	Review the EAS manual to determine the guidelines when using MS tools to process operational personal data and more specifically chapter 8.
Recommendation 14	Analyse the current setup to determine what operational personal data is logged and reflect this in reviewed process descriptions (i.e. document the existing situation).
Recommendation 15	Implement logging of the use of operational personal data on national systems either by having a process to consolidate the existing logs or implementing a solution that provides similar capabilities for auditing.
Deadline:	With regard to recommendation 13, three months after receipt of the report. With regard to recommendations 14 and 15, six months after receipt of the report.

b) Process descriptions for personal data processed in 'DSC not-completed' folders

For each of the inspected OTFs, personal data obtained by Europol via LFE or RSYNC are placed in a 'data subject classification (DSC) not completed' folder at Europol. Europol's current implemented solution for transfer of large files, LFE (Large File Exchange) does not support RSYNC synchronization. However, the processing operations used by RSYNC and LFE are similar: a country will contribute operational information, which cannot be sent via SIENA due to the size, format and frequency.

At the time of the inspection, the DSC mechanism was not clearly described in the Intake Process69 nor in the Operational Analysis Process[70]. The absence of documentation on DSC data may lead to the possible use of unlabelled data in the Article 18(2)(c) operational analysis lifecycle which is identified in the EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorisation[71].

[69] EDOC #968846v2

[70] EDOC #934574v2

[71] https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf

Findings

Finding 20	The DSC mechanism is not clearly described in the relevant processes.

Recommendations

Recommendation 16	The process descriptions should be updated to reflect that the DSC mechanisms are taken into account. The process descriptions should take care to include the necessary controls to ensure that no data without a DSC is used in the operational analysis contrary to the Europol Regulation.
Deadline:	Three months after receipt of the report.

c) Compliance with Article 18(3) of the Europol Regulation and the Opening Decisions of Europol's Analysis Projects

Article 18(3) stipulates that:

(a) for every operational analysis project, the Executive Director shall 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, and shall inform the Management Board and the EDPS thereof;

(b) personal data may only be collected and processed for the purpose of the specified operational analysis project. Where it becomes apparent that personal data may be relevant for another operational analysis project, further processing of that personal data shall only be permitted insofar as such further processing is necessary and proportionate and the personal data are compatible with the provisions set out in point (a) that apply to the other analysis project;

(c) only authorised staff may access and process the data of the relevant project.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Findings

Finding 21	[redacted]

Finding 21 indicates that Europol may have breached Article 18(3)ER. The EDPS has thus decided to open an investigation to ensure compliance with this article.

5. Compiled list of recommendations and deadline for implementation

5.1. List of recommendations

The EDPS recommends that Europol:

Recommendation 1	*Clarify in the Guidelines on the implementation of Article 39 Europol Regulation the scope of application of Article 39. It should be clear that any 'new type of processing operations' refers to any use of new technology (including the use of new IT systems or substantial changes thereto), mechanisms or procedures, regardless of whether the 'new type of processing operation' is part of a well-known (established) process. The 'new type of processing operation' is subject to a prior consultation, in case it presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.*
Recommendation 2	*Raise awareness of Europol's operational staff on the scope of application of Article 39 ER by adding references to the amended Guidelines, to the process description and to the DPIA template. Europol should provide a detailed action plan as to how they intend to fulfil this recommendation within the deadline.*
Recommendation 3	*Amend part 7 of the Guidelines on the implementation of Article 39 Europol Regulation in order to clarify how the methodology for evaluating the risks for the fundamental rights and freedoms of the data subjects is linked to the assessment of whether the threshold for prior notification of Article 39 ER is met.*

Recommendation 4	*Clarify that part 7 of the Guidelines on the implementation of Article 39 Europol Regulation applies also in the ‘internal DPIAs’.*
Recommendation 5	*Raise awareness among Europol’s operational staff on the importance of the scoping of the DPIA and of the way to carry out a risk assessment (including the threshold assessment of whether the requirements of Article 39 ER to launch a prior consultation are met). Europol should provide a detailed action plan as to how they intend to fulfil this recommendation within the deadline.*
Recommendation 6	*Amend the Article 39 ER EDPS prior consultation process description in order to provide for proper documentation of:* *(i) The risk assessment, including the threshold assessment, that triggers (or not) the application of the prior consultation procedure (currently Article 39 ER). The recommendation also refers to ‘internal DPIAs’;* *(ii) the DPF’s advice, in case it differs from the controller’s decision on whether or not the criteria for mandatory prior consultation are fulfilled;*
Recommendation 7	*Reflect these amendments in the Guidelines on the implementation of Article 39 Europol Regulation and on the DPIA template by including a risk assessment table.*
Recommendation 8	*Amend the Article 39 ER EDPS prior consultation process description in order to provide a mechanism to document, also in the context of ‘fast development projects’ (where the validation of the DPIA is not possible), and before the launch of the processing activities:* *(i) the outcome of the threshold assessment (whether the Article 39 ER threshold is met or not - e.g. in the form of a note); and* *(ii) in case the threshold is met, the risk assessment, which will be further detailed in the DPIA.*
Recommendation 9	*Define the performance metrics that will measure the performance of each of the machine-learning models.*
Recommendation 10	*Set required minimum value(s) for performance metrics so that machine-learning models can be considered as reliable enough to be deployed in production.*
Recommendation 11	*Draft a procedure describing how to assess the suitability of machine-learning techniques with the available datasets for a given task defined by a business requirement.*
Recommendation 12	*Perform a data protection impact assessment for the machine-learning models and the Chat Analysis Tool.*
Recommendation 13	*Review the EAS manual to determine the guidelines when using MS tools to process operational personal data and more specifically chapter 8.*
Recommendation 14	*Analyse the current setup to determine what operational personal data is logged and reflect this in reviewed process descriptions (i.e. document the existing situation).*

Recommendation 15	*Implement logging of the use of operational personal data on national systems either by having a process to consolidate the existing logs or implementing a solution that provides similar capabilities for auditing.*
Recommendation 16	*The process descriptions should be updated to reflect that the DSC mechanisms are taken into account. The process descriptions should take care to include the necessary controls to ensure that no data without a DSC is used in the operational analysis contrary to the Europol Regulation.*

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 number 14 and 15** 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

1. EDOC-#1184553-v3- Provide_machine_learning_toolbox_process_(pr_v_2)
2. EDOC-#1170152-v2-EMMA_-Facial_Detection_and_Similarity_Search_DP_Assessment
3. EDOC-#1169951-v2-EMMA_-_Machine_Translation_DP_Assessment
4. EDOC-#1169933-v2-EMMA_-_Image_Similarity_Search_DP_Assessment
5. EDOC-#1169624-v2-EMMA_-_Text_Classification_DP_Assessment
6. EDOC-#1169515-v3-EMMA_-_Robust_Reading_DP_Assessment
7. EDOC-#1169494-v2-EMMA_-_Image_Classification_DP_Assessment
8. EDOC-#1169381-v3-EMMA_-_Named_Entity_Recognition_DP_Assessment
9. EDOC-#1162317-v5-Policy_on_the_development_and_use_of_machine_learning_tools_for_the_purpose_of_operational_analysis
10. EDOC-#1102120-v4-DPIA_RSYNC_transfer_operational_information

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

Documents received on 4 October 2021

1. EDOC-#1183276v10-Progress_report_on_core_capabilities_EU_interoperability_and_IM_Strategy_Implementation
2. EDOC-#1014781v6_NEO_Target_Architecture
3. List and dates of meetings between business owner and DPF

Documents received on 5 October 2021

1. EDOC-#1124467-v1B-NLP_training_of_production_system
2. EDOC-#1127000-v1A-Security_clearance_for_op_EMMA_
3. ML prototype Image Classification Classes
4. EDOC-#1163851-v1-CAT_Backlog
5. EDOC-#1159717-v3-Chat_Analysis_Tool_-_Functional_requirements (002)

Documents received on 7 October 2021

1. EDOC-#1152667-v2-DPIA_OTF_LIMIT
2. EDOC-#1127278-v2-Machine_learning_tool_-_Article_39_ER_EDPS_prior_consultation_and_internal_DPIA_QUESTIONNAIRE
3. EDOC-#1102120-v4-DPIA_RSYNC_transfer_operational_information
4. DPF Compliance Tool_specific entry overview
5. DPF Compliance Tool_specific entry detailed overview exchanges
6. Data Protection Compliance Tool_general overview
7. Audit Logs of iBase (screenshot interface) (002)
8. Audit Logs of LFE (screenshot interface) (002)
9. EDOC -#1179637-v1-Data AI - Procedure and tools to measure performance in machine learning models (002)
10. EDOC -#1175908-v1-Data AI - Bias in AI (002)
11. EDOC -#1127000-v1A-Security clearance for op EMMA_ (002)
12. EDOC -#1124467-v1B-NLP_training_of_production_system (002)
13. EDOC -#1060506-v5-Operational analysis (Art.18.2.c) process - Process Description_(pr.v.3) (002)
14. Copy of EDOC-#1163851-v1-CAT_Backlog (002)
15. EDOC -#1183407-v2-Data AI - Answer to EDPS letter from 03082021 (002)
16. EDOC -#1184553-v3-Provide machine learning toolbox process_(pr.v.2) (002)
17. EDOC-#1159717-v3-Chat_Analysis_Tool_-_Functional_requirements (002)
18. QA - Team C - EDPS Inspection 2021-09 (002)
19. EDOC -#1179854-v1-Data AI - Security measures and controls limiting the access to the Machine Learning environment (002)
20. EDOC-#1127278-v2-Machine_learning_tool_-_Article_39_ER_EDPS_prior_consultation_and_internal_DPIA_QUESTIONNAIRE

Documents received on 17 February 2022

1. EDOC -#1179611-v4-EMMA - Text Classification Model Card
2. EDOC -#1179491-v4-EMMA - Named Entity Recognition Model Card

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