REPORT
ON
INSPECTION AT EUROPOL

Conducted pursuant to Article 47(2) of Regulation (EC) No. 45/2001 and Article 43(4) of Regulation (EU) No. 2016/794

7 May 2018

EDPS
Supervision & Enforcement Unit
and
IT Policy Sector

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**

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team leader, legal officer</td>
</tr>
<tr>
<td>Inspector (legal)</td>
</tr>
<tr>
<td>Inspector (legal)</td>
</tr>
<tr>
<td>Inspector (legal)</td>
</tr>
<tr>
<td>Inspector (IT)</td>
</tr>
<tr>
<td>Inspector (IT)</td>
</tr>
<tr>
<td>Inspector (IT)</td>
</tr>
</tbody>
</table>

**HEAD OF ACTIVITY**

**SUPERVISOR**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIEWIÓROWSKI Wojciech Rafał</td>
<td>Assistant Supervisor</td>
</tr>
</tbody>
</table>
1. Executive summary ................................................................. 5
2. Scope ...................................................................................... 6
3. Methodology ........................................................................... 6
4. Analysis and recommendations - Compliance with Regulation 2016/794 ............. 7
   4.1. Data intake ......................................................................... 7
       4.1.1. Background ................................................................ 7
       4.1.2. Criteria ...................................................................... 8
       4.1.3. Actions and findings .................................................. 9
       4.1.4. Conclusion and recommendations .................................. 14
   4.2. Data processing in Analysis Project Migrant Smuggling .................................. 9
       4.2.1. Background ................................................................ 15
       4.2.2. Criteria ...................................................................... 18
       4.2.3. Actions and findings .................................................. 19
       4.2.4. Conclusion and recommendations .................................. 27
   4.3. Data processing in Analysis Project Heroin .................................................... 29
       4.3.1. Background ................................................................ 29
       4.3.2. Criteria ...................................................................... 31
       4.3.3. Actions and findings .................................................. 33
       4.3.4. Conclusion and recommendations .................................. 37
   4.4. Data review and deletion (technical aspects) .................................................. 38
       4.4.1. Background ................................................................ 38
       4.4.2. Criteria ...................................................................... 38
       4.4.3. Actions and findings .................................................. 39
       4.4.4. Conclusion and recommendations .................................. 44
   4.5. Data review and data deletion (legal aspects) ................................................ 45
       4.5.1. Background ................................................................ 45
       4.5.2. Criteria ...................................................................... 46
       4.5.3. Actions and findings .................................................. 47
       4.5.4. Conclusion and recommendations .................................. 50
   4.6. Information security management ............................................................. 51
       4.6.1. Background ................................................................ 51
       4.6.2. Criteria ...................................................................... 51
       4.6.3. Actions and findings .................................................. 52
       4.6.4. Conclusion and recommendations .................................. 59
   4.7. (technical aspects) .................................................................. 63
       4.7.1. Background ................................................................ 63
       4.7.2. Criteria ...................................................................... 63
4.7.3. Actions and findings ................................................. 63
4.7.4 Conclusion and recommendations .................................. 65

5. Compliance with Regulation 45/2001 of as a monitoring tool - Analysis and recommendations ........................................ 66
   5.1. Background .......................................................... 66
   5.2. Criteria ............................................................... 66
   5.3. Actions and findings ............................................... 67
   5.4. Conclusions and recommendations ............................... 68

6. Compiled list of recommendations and deadline for implementation .................................. 68
   6.1. List of recommendations .......................................... 68
   6.2. Deadline for implementation ...................................... 68
   Annex 1 – Powers of the EDPS ........................................ 75
   Annex 2 – Documents collected during the inspection ................ 77
   Annex 3 – Documents requested during the inspection and communicated afterwards 80
   Annex 4 List of abbreviations ......................................... 81
The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 41 of Regulation (EC) No. 45/2001 (Regulation 45/2001) responsible for:

- monitoring and ensuring the application of the provisions of the Regulation 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 a 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 (Regulation 2016/794 or Europol Regulation), 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 45/2001 applies to Europol’s processing of administrative data.

To these ends, the EDPS fulfils the duties and exercises powers provided for in Articles 46 and 47 of Regulation 45/2001 as well as Article 43 of Regulation 794/2016. 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 the Regulation.

The inspection at Europol was designed to investigate and ensure compliance with Regulation 2016/794 and Regulation 45/2001.

The formal decision was communicated to Europol by means of an Announcement Letter dated 14 November 2017. The fieldwork was carried out between 12 and 15 December 2017 at the Europol premises in The Hague. The minutes of the inspection were sent to Europol for comments on 23 January 2018. Europol communicated their comments on 8 February 2018. The final minutes were sent to Europol on 22 February 2018.

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 to comply with Regulation 2016/794 and Regulation 45/2001. The EDPS will carry out a close follow-up. If need be, powers listed in Annex 1 may be exercised.
This inspection was part of the EDPS annual inspection plan for 2017 and should be viewed as the final stage before formal enforcement action under Article 43(3) of Regulation 2016/794 and Article 47(1) of Regulation 45/2001.

Taking particular account of the new legal framework of Europol, Europol's priority crime areas, issues raised during the first months of its supervision over Europol and conclusions from the last inspection reports of the Joint Supervisory Body (JSB) of Europol, the EDPS determined the scope of the inspection as follows.

**Legal part**

The inspection followed the new approach of Regulation 2016/794 to frame Europol's personal data processing activities, which regulates data uses (cross-checking, strategic/thematic/operational analysis). Specific attention was paid to the processes as well as to the tools used to process personal data and produce intelligence products and services.

Hence, the inspection took into account the whole 'data lifecycle'. In doing this, the EDPS inspection team focused on the following processing activities:

- data intake by the Front Office;
- data processing in the context of two Operational Analysis Projects (AP):
  - AP Migrant Smuggling;
  - AP Heroin;
- data quality and data review/destruction
- in addition: compliance with the provisions of Regulation 45/2001 in the context of the as a system monitoring the activities of Europol staff members.

**Technical part**

The inspection activities covered the following topics:

- Europol's Information security management (selected elements based on ISO 20007-1:2013);
- check on the applications logs of
- retention of data in Europol's systems (Art. 31(2) of the Europol Regulation).

The inspection was performed in accordance with the procedures established in the EDPS Inspection Guidelines 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.

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 2), as well as documents requested during the on-site inspection and provided afterwards (the latter being listed in Annex 3).

A list of abbreviations used in this report is included in Annex 4.

**4.1. Data intake**

**4.1.1. Background**

Intake process

The Front Office (O1) is responsible for data intake and data review assessments. The purpose of the intake process is to determine the legality of the information and the processing purpose according to the Europol Regulation (ER). The outcome of the process is that data are rejected or accepted, labelled and stored correctly as operational, thematic/strategic and cross-checked against the appropriate databases (Europol Information System (EIS), Europol Analysis System (EAS), Schengen Information System (SISII), ...), in anticipation of further processing.

The inspection activities focused on the five possible intake scenarios in the context of contributions sent for purposes of operational analysis, namely:

1. Rejection.
2. Acceptance for the purpose of determining its relevance under Article 18(6) ER or to assign a specific purpose when it cannot be clearly inferred from the contribution (Article 19(1) ER).
3. Acceptance for strategic/thematic analysis (SA/TA) only.
4. Acceptance for SA/TA and Operational analysis (OA).
5. Re-assessment in view of new inputs.
JSB inspection reports

4.1.2. Criteria

The following provisions of the Europol Regulation are of particular relevance in this context:
- Art. 3: Europol's scope of competences, i.e. support of national (Law Enforcement Authorities (LEAs) for the prevention and combatting of serious crimes affecting two or more Member States (MS).
- Art. 4: tasks for which Europol is competent.
- Art. 18: list of legitimate purposes for which Europol can process the data it receives and restrictions attached thereof.
- Art. 19(1): Europol to determine the purpose(s) for which the contributions sent by data providers should be processed if not indicated, in agreement with the data provider.
- Art. 22: obligation to notify MS without delay of any information concerning it.
- Art. 28: general data protection principles.
- Art. 29: obligation to assess of reliability of the source and accuracy of the info.
- Art. 30: restriction of the processing of personal data in respect of victims, witnesses and informants, and minors to cases where it is strictly necessary and proportionate. Restriction of the processing of sensitive data to cases where it is strictly necessary and proportionate and if they supplement other personal data processed by Europol.
- Art. 31: time limits for data storage.
- Annexes I and II: categories of data and categories of data subjects whose data which can be processed for each purpose of Art. 18.
The following Europol’s internal documents were also considered:

- The Integrated Data Management Concept (IDMC) Guidelines adopted by the Management Board of Europol on 13 December 2017 in accordance with Article 18(6) and (7) ER14;
- The IDMC Guidelines Specification15;
- IDMC Quick wins and urgent requirements16;
- Integrated data management concept. Further elaboration of processing purposes17;
- Input Manual18;
- Processing and handling procedure for basic support cases19;
- Manual for assessing contributions - Operational Centre20;
- Intake process description21;
- Briefing Note: Road map for improving data quality & data protection compliance in Europol's Analysis Work Files (AWF)22;
- Europol, New AWF Concept, Guide for MS and Third Parties, 31 May 201224;

4.1.3. Actions and findings
4.2. Data processing in Analysis Project Migrant Smuggling

4.2.1. Background
Victims of trafficking of human beings (THB)

The JSB pointed out to Europol that "in view of the victim-centred approach and the importance of recognizing the vulnerable position of victims, a controller should in these situations put the emphasis on the aspect of THB which must be protected with priority: the victim."\(^{64}\)

These considerations are consistent with Article 8 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims\(^{67}\), stating that "Member States shall, in accordance with the basic principles of their legal systems, take the necessary measures to ensure that competent national authorities are entitled not to prosecute or impose penalties on victims of trafficking in human beings for their involvement in criminal activities which they have been compelled to commit as a direct consequence of being subjected to any of the acts referred to in Article 2."

Preamble 14 of Directive 2011/36/EU also highlights that: "Victims of trafficking in human beings should, in accordance with the basic principles of the legal systems of the relevant Member States, be protected from prosecution or punishment for criminal activities such as the use of false documents, or offences under legislation on prostitution or immigration, that they have been compelled to commit as a direct consequence of being subject to trafficking. The aim of such protection is to safeguard the human rights of victims, to avoid further victimisation and to encourage them to act as witnesses in criminal proceedings against the perpetrators. This safeguard should not exclude prosecution or punishment for offences that a person has voluntarily committed or participated in." (emphasis added).
Compliance report of the Data Protection Function (DPF) of Europol

In September 2017, the DPF unit issued a compliance report on personal implications in the new EAS (Palantir).

AP Migrant smuggling was stored on at the time of the inspection. However, all ex SOC FPs were scheduled to migrate to Palantir during the first trimester 2018.

Statistics on data on special categories of data subjects and sensitive data

According respectively to Articles 30(6) ER and 31(3) ER, Europol must:

- provide every year to the EDPS a statistical overview of sensitive data it has processed;
- inform the EDPS if sensitive data and data about special categories of data subjects are stored for a period exceeding five years.

4.2.2. Criteria

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

- Art. 18(3) and (4): Processing for the purpose of operational analysis;
- Art. 28: General data protection principles;
- Art. 29: Assessment of reliability of the source and accuracy of the information;
- Art. 30: Processing of special categories of data and of different categories of data subjects;
- Art. 31: Time-limits for storage and erasure;
- Annex II.B. - Categories of personal data and categories of data subjects whose data may be processed for the purpose of analysis of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information as referred to in points (b), (c) and (d) of Article 18(2).

The following Europol’s internal documents were also considered:

- The IDMC guidelines adopted in accordance with Article 18(6) and (7) ER;
- IDMC - Quick wins and urgent requirements including notably rules on data review;
- The portfolio of APs, in particular the general section and the Opening Decision (OD) of the AP Migrant Smuggling;
The EDPS also refers to the following documents issued by the JSB:

- Handbook for the transmission of personal data to Europol, providing guidance to the Europol National Units (ENUs);
- Report on “Victims of trafficking in human beings, a data protection perspective” (October 2015).

Finally, the EDPS refers to the following case:

- EDPS case 2015-0346, EDPS prior-checking Opinion on PeDRA (Personal Data in Risk Analysis) regarding notably transfers of personal data on smugglers from Frontex to Europol.

4.2.3. Actions and findings
<table>
<thead>
<tr>
<th>No.</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommendations concerning AP Migrant smuggling</strong></td>
<td>Ensure that the allocation of human resources of Unit O27 is consistent with its workload to ensure a timely and accurate data review process in coordination with Unit 053.</td>
</tr>
</tbody>
</table>

| **General recommendations on the new EAS** | Ensure, with reference to APs migrated to the new EAS (Palantir), that each person inserted in EAS has a personal implication. Ensure that the personal qualification is a mandatory field of Palantir’s data model. |
### Recommendations

<table>
<thead>
<tr>
<th>No.</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Revise Palantir’s data model to include <strong>mandatory fields for special categories of personal data</strong> where (and only where) such personal data (if allowed by the OD of the AP) can be inserted.</td>
</tr>
</tbody>
</table>

### 4.3. Data processing in Analysis Project Heroin
4.3.2. Criteria
The following provisions of the Europol Regulation are of particular relevance in this context:

- Art. 18(3) and (4) – Processing for the purpose of operational analysis;
- Art. 28 – Data protection principles;
- Art. 29 – Assessment of reliability of the source and accuracy of the information;
- Art. 30 – Processing of special categories of data and of different categories of data subjects;
- Art. 31 – Time-limits for storage and erasure;
- Annex II. B. – Categories of personal data and categories of data subjects whose data may be processed for the purpose of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information as referred to in points (b), (c) and (d) of Article 18(2).

The following Europol’s internal documents were also considered:

- IDMC guidelines adopted in accordance with Article 18(6) and (7) ER;
- Portfolio of APs\textsuperscript{131}, in particular the general section and the opening decision (OD) of AP Heroin;
- input Manual\textsuperscript{132};

- Road map for improving data quality & data protection compliance in Europol’s AWF of 25 February 2016\textsuperscript{135} in particular the following issues:
As regards Palantir ontology (personal implication, specific fields for each category of sensitive data), the EDPS refers to above-mentioned recommendations.
4.4. Data review and deletion (technical aspects)

4.4.1. Background

The inspection activities were focused on reviewing the time limits for the storage and erasure of personal data according to Articles 28(1)(e) and 31 ER and more specifically how these limits have been applied to the critical operational systems of Europol, mainly SIENA, the EIS and the EAS. During the inspection, EAS had two running versions 2.0 ( ) and 3.0 (Palantir).

The inspection team interviewed Europol officials that are mainly responsible as product managers for these systems.

4.4.2. Criteria

Article 28(1)(e) ER states that personal data shall be kept in a form which permits identification for as long as is necessary and proportionate for the purposes for which the data are processed.

Article 31 ER defines the time-limits for the storage and erasure of personal data. According to that provision:

- data should be kept only for as long as necessary, and proportionate to the purposes for which it is processed.
- No later than three years, the continued storage must be reviewed. If no decision is taken about the review, the data must be erased automatically after three years.

These provisions trigger the obligation for Europol to assess the need for continued storage if circumstances arise which suggest that the data have to be deleted [or corrected].172

Article 31(3) ER imposes on Europol the obligation to inform the EDPS if personal data are stored for a period exceeding five years (and, even though not expressly stated by the legislator,
to assess proportionality of the data processing beyond the five years in accordance with the
general data protection principles of necessity and proportionality laid down under Articles
28(1)(e) and 31(1) ER.

Article 18(6) ER allows the temporary processing of data, including personal data, but
establishes a retention time-limit of six months. Before the end of that period, data must be
erased or allocated to another purpose referred to under Article 18 ER.

The following Europol’s internal documents were also considered:

• Europol Data Archiving Policy\textsuperscript{178};
• SIENA Use and Management policy\textsuperscript{179};
• SIENA Data Retention Policy\textsuperscript{180}.
4.5. Data review and data deletion (legal aspects)

4.5.1. Background

Unit O53 is the Unit in charge of the data review and deletion process. It streamlines the process, ensuring consistency across the Units in charge of the APs and directly performs the deletion of data (at a 'centralised level') for all APs on the basis of the assessment made by the analysts of the APs\textsuperscript{186} (and the feedback from Member States law enforcement authorities). In this section we will focus on some main strategic trends regarding the data review process. The inspection activities focused on the following data processing scenarios\textsuperscript{187}:
1) data stored for temporary processing (maximum six months) to determine relevance under Article 18(6) ER;
2) the three-year review: data stored in EAS for operational analysis and/or for strategic and thematic analysis;
3) special categories of personal data\textsuperscript{188} and of data subjects\textsuperscript{189} stored for more than five years: this scenario does not trigger a legal obligation for Europol to conduct a review\textsuperscript{190}. If such personal data are stored for more than five years, Europol must inform the EDPS\textsuperscript{191}. The AWF manual\textsuperscript{192} provides that the processing of special categories of personal data and of data subjects is one of the criteria that may trigger ad hoc data reviews.

The JSB January 2017 inspection report contains recommendations on data review and deletion\textsuperscript{193}.

The EDPS inspection activities did not cover the data review and deletion procedures in the EIS.

4.5.2. Criteria

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

- Art. 18(3) and (4) – Processing for the purpose of operational analysis;
- Art. 18(6) – Temporary processing of personal data for the purpose of determining their relevance;
- Art. 28 – Data protection principles;
- Art. 29 – Assessment of reliability of the source and accuracy of the information;
- Art. 30 – Processing of special categories of data and of different categories of data subjects;
- Art. 31 – Time-limits for storage and erasure;
- Annex II.B. – Categories of personal data and categories of data subjects whose data may be processed for the purpose of analysis of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information as referred to in points (b), (c) and (d) of Article 18(2).

The following Europol's internal documents were also considered:
- AWF Manual, Section 5\textsuperscript{194};
- briefing note: Updated operational data review process (7/10/2016)\textsuperscript{195}
- IDMC – Quick wins and urgent requirements, section 3 – data review, 16 October 2017\textsuperscript{196}
- briefing note on special categories of personal data (6/11/2017)\textsuperscript{197}
- processing and handling procedures for basic support cases\textsuperscript{198}
- briefing note. Road map for improving data quality and data protection compliance in Europol AWF\textsuperscript{199};
- manual for assessing contributions. Operational centre\textsuperscript{200}.

4.5.3. Actions and findings
4.6. Information security management

4.6.1. Background

The need to maintain the integrity of information and to protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies and procedures. Security management also includes performing security monitoring, periodic testing and implementing corrective actions for identified security weaknesses or incidents.

The objective of the information security management review is to:

- provide Europol management with an assessment of the effectiveness of the information security management function.
- Evaluate the scope of the information security management of Europol and determine whether essential security functions are being addressed effectively.

4.6.2. Criteria

Two main criteria justify checking the overall information security management at Europol. Firstly, the topic was inspected by the JSB back in 2000. After that, the JSB did not inspect again the information security management system at Europol, but rather focused on specific technical topics. Since then, the Europol infrastructure has evolved and many new policies on security have been drafted.

Secondly, information security management is an important element of the security of processing and it is related to the following provisions of the Europol Regulation:

- Recital 45;
- Article 32 on security of processing;
- Article 34, 35 and 36 on personal data breaches

The following Europol's internal documents were also considered:

- Information security risk management process;
- Europol Operations Network Use Policy;
- Europol Security Manual;
5.1. Background

Europol developed the DPF to comply with Article 40 of the Europol Regulation (Logging and documentation). Through the DPF, the DPF also verifies the lawfulness of data processing by Europol staff. The EDPS inspection activities aimed to verify the DPF’s compliance with Regulation 45/2001. Indeed, the DPF’s monitoring of Europol’s staff activities relates to administrative personal data and therefore falls within the scope of Regulation 45/2001.

5.2. Criteria

Relevant provisions of Regulation 45/2001, identification of DP risks:

- Right of information, Articles 11 and 12 of the Regulation;
- Retention periods, Article 4(1) of the Regulation.

Other reference documents:

- Road map for improving data quality and DP compliance in AWFs;
- Overall requirements;
- Data protection statement.
5.3. **Actions and findings**
5.4. Conclusions and recommendations

Taking into account the findings reported above, the EDPS recommendations are as follows:

<table>
<thead>
<tr>
<th>No.</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Inform all users</strong> through an easily accessible specific data protection statement about the possible processing of their personal data by the before they start using the audited databases. In particular, such information should be provided for users of Palantir and SIENA. For instance, a link to the Privacy statement could appear on the entry page to Palantir and SIENA and once logged in.</td>
</tr>
<tr>
<td></td>
<td>If the DPF were to use the <strong>audit the auditor function</strong>, inform all DPF staff members about the possible processing of their personal data through the specific data protection statement before they use the . The DPF shall ensure the exercise of the rights of access and rectification.</td>
</tr>
</tbody>
</table>
Annex 1 – Powers of the EDPS

Art 47 of the Regulation 45/2001 sets forth the powers of the EDPS as follows:

"...
1. The European Data Protection Supervisor may:

(a) give advice to data subjects in the exercise of their rights;
(b) refer the matter to the controller 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 13 to 19;
(d) warn or admonish the controller;
(e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;
(f) impose a temporary or definitive ban on processing;
(g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;
(h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;
(i) intervene in actions brought before the Court of Justice of the European Communities.

2. The European Data Protection Supervisor shall have the power:

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

...

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.

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 4  List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFIS</td>
<td>Automated Fingerprint Identification System</td>
</tr>
<tr>
<td>AP</td>
<td>Analysis Project</td>
</tr>
<tr>
<td>AWF</td>
<td>Analysis Work File</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CMR</td>
<td>Cross-match report</td>
</tr>
<tr>
<td>CORPNET</td>
<td>Corporate network</td>
</tr>
<tr>
<td>CT</td>
<td>Counter terrorism</td>
</tr>
<tr>
<td>DPF</td>
<td>Data Protection Function unit</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>EAS</td>
<td>Europol Analysis System</td>
</tr>
<tr>
<td>EDOC</td>
<td>Europol Document</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EIS</td>
<td>Europol Information System</td>
</tr>
<tr>
<td>EMPACT</td>
<td>European Multidisciplinary Platform Against Criminal Threats</td>
</tr>
<tr>
<td>EMSC</td>
<td>European Migrant Smuggling Centre</td>
</tr>
<tr>
<td>ER</td>
<td>Regulation 2017/94 (Europol Regulation)</td>
</tr>
<tr>
<td>FP</td>
<td>Focal Point</td>
</tr>
<tr>
<td>GNST</td>
<td>General Nature and Strategic Type</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity Access Management interface</td>
</tr>
<tr>
<td>IDMC</td>
<td>Integrated Data Management Concept</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITOC</td>
<td>IT Operational Centre</td>
</tr>
<tr>
<td>JSB</td>
<td>Europol Joint Supervisory Body</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>LEAs</td>
<td>Law Enforcement Authorities</td>
</tr>
<tr>
<td>MS</td>
<td>Member State</td>
</tr>
<tr>
<td>O1</td>
<td>Europol Front Office</td>
</tr>
<tr>
<td>OA</td>
<td>Operational Analysis</td>
</tr>
<tr>
<td>OAR</td>
<td>Operational Analysis Report</td>
</tr>
<tr>
<td>OCG</td>
<td>Organised Crime Group</td>
</tr>
<tr>
<td>OD</td>
<td>Opening Decision</td>
</tr>
<tr>
<td>OO</td>
<td>Opening Order</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>PeDRA</td>
<td>Personal Data in Risk Analysis</td>
</tr>
<tr>
<td>QUEST</td>
<td>Querying Europol Systems</td>
</tr>
<tr>
<td>SA</td>
<td>Strategic Analysis</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SIENA</td>
<td>Secure Information Exchange Network Application</td>
</tr>
<tr>
<td>SIS</td>
<td>Schengen Information System</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SOC</td>
<td>Serious and Organised Crime</td>
</tr>
<tr>
<td>SOCTA</td>
<td>Serious and Organised Crime Threat Assessment</td>
</tr>
<tr>
<td>SSSR</td>
<td>System Specific Security Requirements</td>
</tr>
<tr>
<td>TA</td>
<td>Thematic Analysis</td>
</tr>
<tr>
<td>THB</td>
<td>Trafficking of Human Beings</td>
</tr>
<tr>
<td>TP</td>
<td>Third Party</td>
</tr>
<tr>
<td>USE</td>
<td>Unified Search System</td>
</tr>
</tbody>
</table>