EDPS EUROPEAN DATA PROTECTION SUPERVISOR

Case Reference
2018-0067

REPORT ON INSPECTION AT EUROPOL

Conducted pursuant to Article 47(2) of Regulation (EC) No. 45/2001[1] and Article 43(4) of Regulation (EU) No. 2016/794

19 December 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

	Team leader, Inspector (legal)
	Inspector (legal)
	Inspector (legal)
	Inspector (legal)
	Inspector (IT)
	Inspector (IT)
	Inspector (IT)
	Inspector (Legal)
	Inspector (IT)

HEAD OF ACTIVITY INSPECTIONS

SUPERVISOR

WIEWIÓROWSKI Wojciech Rafał	Assistant Supervisor

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of Regulation 2018/1725[2] [3]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[4] (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 2018/1725 (formerly Regulation 45/2001) applies to Europol's processing of administrative data[5].

To these ends, the EDPS fulfils the tasks and exercises powers provided for in Articles 57 and 58 of Regulation 2018.1725[6] 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 2018/1725.

The formal decision was communicated to Europol by means of an **Announcement Letter** dated 10 April 2018. A **pre-inspection meeting** took place on 24 April 2018. The **fieldwork** was carried out between 22 and 25 May 2018 at the Europol premises in The Hague. The **minutes** of the inspection were sent to Europol for comments on 25 June 2018. Europol communicated their comments on 18 July 2018. The final minutes were sent to Europol on 27 July 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 2018/1725. 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 2018 and should be viewed as the final stage before formal enforcement action under Article 43(3) of Regulation 2016/794 and Article 58 of Regulation 2018/1725.

The inspection focused on data processing activities which were not covered by the previous inspection, or which were brought to the attention of the EDPS in the course of supervisory activities conducted during the first year of the supervision of Europol. The EDPS also took into consideration recommendations from the last inspections of the Joint Supervisory Body (JSB) of Europol.

Consequently, the EDPS determined he scope as follows.

Legal part (Regulation 2016/794)

1. Europol Information System (EIS);
2. Secondary security checks at migration "hotspots" in Greece and Italy;
3. Processing of personal data on persons under 18 in the Europol Analysis System (EAS);
4. Data processing in the context of the Analysis Project Travellers.

Technical part (Regulation 2016/794)

5. Palantir Gotham (Palantir), the new EAS;

7. Information security management – Business continuity management and User account management;

Administrative data (Regulation 45/2001, now Regulation 2018/1725)

9. Selection and recruitment procedures.

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[7].

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**).

A list of **abbreviations** used in this report is included in **Annex 3**.

4.1. Europol Information System

4.1.1. Background

The Europol Information System (EIS) is the Europol central criminal information database. It covers all of Europol's mandated crime areas and contains information on suspected and convicted persons, as well as persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State (MS) concerned to believe that they will commit criminal offences in respect of which Europol is competent ('Potential future criminals'); criminal structures; offences and the means used to commit them. It is **a reference system** that can be used to check whether information on a certain person or an object of interest (such as a car, a telephone or an e-mail message) is available beyond national or organizational jurisdictions.

The data in the EIS is stored within different online 'entities' corresponding to actual objects such as cars and identity documents, and to people. The online 'entities' can be linked to each other in different ways as to create a structured picture of a criminal case.

Data inserted into the EIS database is under the **control of the MS which provide the personal data to Europol** (MS are data owners) and cannot be altered in any way by Europol or another MS. Third parties (TP) may also request Europol to insert data in the EIS.

The responsibility in data protection matters between Europol and MS is as follows, according to Regulation 2016/794 (Europol Regulation or ER).

MS that insert data in the EIS are responsible in particular for:

- the accuracy of information and the reliability of the source of the information (Article 29 ER);
- the quality of the personal data (Article 38 (2) (a) ER);
- the legality of the transfer of data to Europol (Article 38(5)(a) ER).

Europol is responsible for:

- inserting in the EIS and checking the **quality** of personal data provided by **third countries or international organisations** or directly provided by private parties, as well as of personal data retrieved by Europol from publicly available sources or resulting from Europol's own analyses, and of personal data stored by Europol in accordance with Article 31(5) ER[8] (Article 38(2)(b) ER);
- **informing** either the data owner or other data provider of any potential **inaccuracy** in case that it becomes aware that some personal data provided are factually incorrect or have been unlawfully stored (Article 38(3) ER);
- complying with the principles of **fair and lawful processing, purpose limitation, data minimisation, retention and appropriate security** (Article 38(4) ER).

In December 2017, the EDPS inspected the information technology and security aspects of the EIS, which included data retention and its subsequent deletion.[9] The present inspection focuses on legal aspects of the EIS and especially on data quality.

4.1.2. Criteria

Unlike the former Europol Council Decision (ECD), and following the IDMC[11] approach the ER does not expressly mention the EIS but sets out conditions and limits for processing personal data for the purpose of **cross-checking** in Articles 18(2)(a), Article 20 and Annex II.A of the ER. These provisions apply to the EIS as far as it is a source for cross checking.

The processing of personal data by Europol for the purpose of cross-checking is limited to the categories of data subjects and personal data which are specified in Annex II. A, of the ER, i.e. **suspects, convicted persons and potential future criminals**.

Additional rules on cross-checking are set out in Article 5 of the IDMC Guidelines[12] as well as in the EIS Use and Management Policy.

4.1.3. Actions and findings

During the on-site activities, the inspection team (team A) met

The interviews were followed by practical demonstrations. A member of the Data Protection Function (DPF) unit was present throughout the on-site activities.

All inspection activities are described in detail in the inspection minutes.[13] This section focuses on the most relevant inspection activities and in particular on these which gave raise to findings and recommendations.

a. *Data quality checks - Inconsistencies between data in the EIS and in the Europol Analysis System (EAS)*

Several entities, i.e. the Operations Department (O1) and the Capabilities Directorate Business Product Management (CDBPM) **share responsibility** for data quality in the EIS. Quality checks are performed by O1 and by the DPF. pointed out that there is a **lack of resources** available for quality checks.

As highlighted above, Europol is not responsible for the data inserted by MS in the EIS. If Europol becomes aware of any inconsistency concerning a given person, they inform the MS concerned and ask them to reconsider the data.[14]

In this context, inconsistencies may arise between the EIS and the EAS regarding **victims of trafficking in human beings** (THB). Indeed, these persons are often involved in criminal activities which they are compelled to commit as a direct consequence of being subject to THB. As a consequence, they may be labelled as victims in the EAS (AP Phoenix) and as suspects in the EIS. Europol performed a specific check on victims of THB in May 2018 and found that the same persons appeared as *suspects* in the EIS and as *victims/witnesses* in the EAS. Thus, Europol asked the competent authorities of the countries concerned to review the insertion of these persons in the EIS. [15]

4.2. Secondary Security Checks at Hotspots

4.2.1. Background

The '**hotspot approach**' was set up as part of the European Agenda for Migration[40], presented by the European Commission (EC) in May 2015. Following this agenda COM set up a new 'hotspot' approach, where the European Asylum Support Office (EASO), Frontex and Europol

work on the ground with frontline MS to swiftly identify, register and fingerprint incoming migrants. The work of the agencies is complementary to one another. Those claiming asylum are immediately channelled into an asylum procedure where EASO support teams will help to process asylum cases as quickly as possible. For those not in need of protection, Frontex helps MS by coordinating the return of irregular migrants. Europol and Eurojust assist the host MS with the investigation to dismantle smuggling and trafficking networks.

There is **no specific legal framework** setting up the activities of Europol at the hotspots. The activities of Europol staff (actually seconded national experts) in the hotspots are governed by the Europol Regulation.

Europol describes their activities in the hotspots as follows[41]:

'Although tasks like this [Europol's operational support at the hotspots] are not specifically foreseen in the Europol Council Decision, nor for that matter considered in discussions on the recent Europol Regulation, we consider that Article 3 Europol Council Decision[42] (ECD) provides the relevant legal basis for this mission (and Article 39(5) ECD[43] in terms of SNEs (Seconded National Experts).

Under the corresponding current legal framework, Article 3 of the ER states that: 'Europol shall support and strengthen action by the competent authorities[46] of the Member States and their mutual cooperation in preventing and combating serious crimes affecting two or more MS, terrorism and forms of crime which affect a common interest covered by a Union policy, as listed in Annex I.' Article 36 ER states that Europol may make use of seconded national experts.

In the context of the hotspot activities, Europol's Guest Officers (GOs) aim to play a role in the prevention of terrorism and other crimes falling under Europol's mandate, such as smuggling of migrants and THB. They work closely with Europol's specialised centres: the European Counter Terrorism Centre (ECTC) and the European Migrant Smuggling Centre (EMSC). In

41 Europol "FAQ regarding Guest Officers (GO)", 22 August 2016, EDOC#844691v8.

42 Article 3 ECD: "The objective of Europol shall be to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States. For the purposes of this Decision, 'competent authorities' shall mean all public bodies existing in the Member States which are responsible under national law for preventing and combating criminal offences."

43 Article 39(5) ECD: "Member States may second national experts to Europol. The Management Board shall adopt the necessary implementing arrangements for that purpose."

46 The definition of "competent authorities" under Article 2(a) ER is: "all police authorities and other law enforcement services existing in the Member States which are responsible under national law for preventing and combating criminal offences. The competent authorities shall also comprise other public authorities existing in the Member States which are responsible under national law for preventing and combating criminal offences in respect of which Europol is competent".

practice, **Europol GOs** placed at hotspots **facilitate the communication between hotspots and Europol's headquarters.**

These requests aim to conduct **security checks** on selected individuals arrived at the hotspots. When GOs receive a referral, they perform a first check of the person in all Europol's databases through their mobile office[47] and also consult via SIENA the Europol Support Team at Europol headquarters, by attaching the request of referral to the SIENA message. The GOs inform the contact point of about the result of the search (hit/no hit) whereas the official result of the cross-checking is sent via SIENA to the relevant Europol national unit (ENU).

Each Operational Plan describes in particular:

- the **information** flows between Europol staff and national authorities;
- the procedures to be followed by Europol in case of **'no hit'** (in particular the storage under Article 18 (6) ER of data cross-matched by Europol and the deletion of these data after six months);
- the procedures to be followed in case of **'hit'** (in particular storage of data by Europol in the relevant database with handling code H2[50], notice to national competent authority, possible lifting of the H2 code by the competent authority and notice of the hit by Europol to the involved MS).

Europol provided **statistics** covering the last three years, for each hotspot as regards:

- the number of requests for referrals for secondary security checks;
- the number of checks performed by Europol against their databases;

- the number of cases referred for forensic support.

4.2.2. Criteria

The most relevant documents concerning the role of Europol staff at the hotspots are **the Operational Plan**, adopted by Europol Management Board.

The wording 'appropriate' of the OP entail *inter alia* that checks against Europol databases should not be done on a routine basis. Routine checks on migrants against Europol databases are not foreseen either by the ER or any other legal basis. There is thus **no legal basis allowing for routine checks of migrants crossing the EU borders at hotspots.**

The following **provisions of the ER** are relevant in this context:

- Article 28 (1) on general data protection principles;
- Article 30 on processing of special categories of personal data and different categories of data subjects;
- Article 40 on logging and communication.

The inspection team also examined the data processing activities in light of the **DPF audit report of September 2017**[55] which found a number of critical items regarding the processing operation at stake, in particular, relating to the following aspects:

- Given the lack of legal basis, systematic checks by Europol GOs are not allowed[56];

55 Audit Report, "Guest officers data processing activities", September 2017, EDOC#911031v3.

- There is no clarity as to the sharing of tasks and duties between GOs and national local authorities[57];
- The quality of the referrals should be examined.

4.2.3. Actions and findings

The inspection team (team A) met the Head of Counter Terrorism (CT) Operations, the Manager of the initiative a Senior Analyst two Analysts from one Analyst from as well as a GO Officer from European Union Regional Task Force (EURTF) Greece who participated to the interview via video-conference. The interviews were followed by practical demonstrations.

A member of the DPF unit was present throughout the on-site activities.

All inspection activities are described in detail in the inspection minutes.[58] This section focuses on the most relevant inspection activities and in particular on activities which triggered findings and recommendations.

a) Applicable rules

Hotspots activities are dealt with by different units and teams of Europol,
The procedures in place for secondary security checks are described in different documents
Finally, some indications on quality control are pointed out

There is thus certain dispersity given the different documents applicable as well as different teams involved.

According to Europol, staff members of the two teams responsible for hotspots systematically collaborate. They have a good cooperation and provide training and mentoring to GOs before they start their activities. Where there is a request for referral or an issue at hotspots, the staff members of the two teams always discuss between them who 'takes cases on board' and usually there is a good understanding between the two teams.
was historically on the lead on activities related to hotspots. Experience showed that many persons involved in terrorism activities were going through hotspots
Both teams currently work together establishing 'who does what' in a natural way.

58 See inspection minutes, pp. 15-32.

Europol has no objection in principle to a certain formalization of tasks and duties, including workflows, quality checks, insofar as this does not lead to excessive rigidity for operations activities.

Considering that there is no specific legal framework and that the activities of GOs are remote from Europol's headquarters, the EDPS recommends that Europol adopt a formal **comprehensive policy document** that would:

- clarify who does what in the field of hotspots, by identifying tasks and duties of Europol staff and division of tasks between Europol GOs and LEAs;
- contain workflows, data quality reviews, standard models on requests for referrals, etc.

As a suggestion Europol could prepare this comprehensive policy on the basis of which, according to the DPF audit report, is still at a draft stage. In addition it could also integrate the policy the indications contained in

b) Security checks outside the hotspots

As Europol's processing activities in mobile hotspots imply additional risks for individuals

Europol should **consult the EDPS** on these potential future activities prior to their implementation, so that the risk can be assessed and appropriate data protection safeguards can be put in place where needed.

c) Identification of vulnerable persons

d) Proactive checks and interventions

e) Criteria for the requests for referrals

The **DPF audit report** highlighted that there is no **legal basis for the secondary security checks** if they are intended **as routine checks**.

The **statistics** on the number of requests for referral provided by Europol show the following:

- the total number of persons submitted to secondary security checks by GOs in Greece for the year 2016 plus the first quarter 2017 is 10.718 out of 40.829 arrivals;
- the total number of persons checked in Italy for the same period is 4.371 out of 37.290.

In light of these statistics, Europol specified that it checks **between 10 and 20%** of the persons arriving.

the reply of Europol to the DPF audit report, as well as statistics from on the ratio of suspects-arrivals for Greece showing a decrease of this ratio, from 62.9% for Q4 2016 to **12,9% for Q4 2017** -but also showing an increase to **15,6%** for Q1 2018.

Thus, as a result of the DPF actions (audits, awareness raising, monitoring via the Unified Audit System), the percentage of secondary security checks performed by Europol (ratio: checks made/persons landed) has **decreased**.

The EDPS takes good note and appreciates the fact that the DPF is taking measures to ensure that requests for referrals are performed only in cases of suspected crimes falling under Europol's mandate) as well as for those cases where there are risk factors indicated All of this has reduced the number of requests for referrals which should increase data quality. Nonetheless, this ratio seems still too high and therefore recommends that Europol further define **criteria for requests for referral.** If criteria are well defined, this should further decrease the number of persons referred to for secondary security checks working together with the national competent authorities on this issue.

f) Quality of the requests for referral

As a positive trend concerning **the quality of the referrals**, the EDPS notes that, going from the oldest to more recent ones, referrals are **increasingly targeted and justified**, providing information on the reasons and circumstances under which GOs decided to perform a referral. The quality of referrals has also increased due to audit and awareness raising performed by the DPF.

Europol teams involved in the hotspot activities and the DPF should **continue working hand-by-hand on the quality of requests for referrals and enhance the positive trend**. In doing so, both Europol and the local LEA shall apply the 'guidelines'

In particular, 'GOs should **reject** a referral when the information provided is insufficient to justify a secondary security check.'

4.2.4. Conclusion and recommendations

In view of the findings reported above, the processing operation of personal data in hotspots by Europol is gradually evolving, also as a result of the careful and efficient actions taken by the DPF. It is evolving towards a situation that can be considered 'overall compliant' with the ER. In order to further reduce the risks of breach of the ER by Europol in the context of the aforesaid activities, the EDPS makes the following recommendations:

Recommendations	
No.	**Content**
7.	Adopt a formal comprehensive **policy regarding Europol's role and tasks at hotspots** (which could be based on 'Hotspot Reporting Guidelines - Referral Letters', which is at a draft stage). This policy should govern the performance of activities by Europol in the context of the migration 'hotspots (in particular, concerning the allocation of tasks and duties, workflows, standard formats, establishment of quality control reviews for accepting the requests for referrals).
8.	**Consult the EDPS** on Europol's **future planned activities** in the context of so-called **mobile hotspots** in order to assess the risks to the fundamental rights and freedoms of the persons concerned and identify the appropriate data protection safeguards.
9.	Add to point 4.1 of the Operational Plans with Greece and Italy a reference to the **victims of THB**.
10.	Further define **criteria for requests for referrals,** in cooperation with the national authorities with a view to narrowing down the ratio secondary security checks per persons landed.
11.	Europol teams responsible for hotspot activities should continue to work on the **quality of requests for referrals,** by applying the guidelines indicated in section 3 of the "Briefing note: guest officer's concept reporting background and guidelines of 19 April 2018". In particular, GOs should **reject** a referral in those cases where the indications are not sufficient to justify a secondary security check. The DPF should continue to **monitor** the data processing activities by the GOs in this respect.

4.3. Processing of persons under 18 in the Europol Analysis System

4.3.1. Background

JSB inspection reports

As mentioned in the ENUs handbook, drafted by the JSB to clarify to MS the rules applicable to the personal data sent to Europol: *The JSB always paid specific attention to the processing of personal data about persons under 18, as they are a vulnerable group of data subjects, even if the Europol Council Decision (ECD) did not contain any specific provision regulating such processing. On the basis of the findings of successive inspections, the JSB identified a list of criteria to be implemented by Europol and by Member* States.

Europol's Portfolio containing the Opening Decisions of the Operational Analysis Projects

For every operational analysis project (AP), Europol must define the specific purpose, categories of personal data, data and categories of data subjects, participants, duration of storage and conditions for access, transfer and use of the data concerned[66]. These rules are included in a Portfolio containing the Opening Decisions (OD) of the APs[67] (the Portfolio).

The Europol Regulation has introduced specific requirements for the processing of personal data about persons under 18. Under Article 30(1) ER, Europol can only process personal data about persons under 18 if these are necessary and proportionate for preventing or combatting crimes that fall within Europol's objectives.

As a result, Europol included rules on the matter in the Portfolio. The Introductory chapter now specifies the criteria used by Europol to ensure that the processing of data about persons under 18 is necessary and proportionate. In addition, a specific justification for the processing of persons under 18 was added in the OD of the APs in which Europol processes data about persons under 18 who are not suspects, convicted persons or potential future criminals. As a result, six ODs [68] were modified: Check The Web, Core International Crimes, Hydra, Phoenix, Travellers, Twins. We reproduce here the content of the justification provided.

> **Check the Web (CTW)**: Operational analysis in the context of this AP is performed to support participants preventing and combating **jihadist propaganda online**. The processing of personal data of persons under 18 is justified

Core International Crimes (CIC): Operational analysis in the context of this AP is performed to support participants in preventing or combating illicit activities of individuals, groups, networks and organisations involved in **genocide, crimes against humanity and war crimes**. The processing of personal data about persons under 18 is justified

Hydra: Operational analysis in this AP is performed to support participants in preventing and combating crimes committed or likely to be committed in the course of **terrorist activities** against life, limb, personal freedom or property, and related criminal offences associated with terrorism perpetrated by individuals, groups, networks or organisations **that evoke Islam to justify their action**. The processing of personal data about persons under 18 is

Phoenix: Operational analysis performed in the context of this AP is performed to support participants in preventing and combating **trafficking in human beings**. The processing of personal data of persons under 18 is justified

Travellers: Operational analysis taken place in the AP Travellers is performed to support competent authorities of the participants to the AP in preventing or combating terrorism by sharing analysis on related **travel activities to terrorist hotspots** (e.g. conflict zones and training venues). The processing of personal data about persons under 18 is

Twins: Operational analysis in the context of this AP is performed to support participants in preventing and combating the activities of criminal networks involved in **sexual exploitation of children**. The processing of personal data about persons under 18 is justified

4.3.2. Criteria

Applicable provisions of Europol Regulation

- Article 30 (1) restricts the processing of personal data in respect of persons under 18 where this is strictly necessary and proportionate for preventing and combating crime that falls within Europol's objectives;
- Article 30 (3) limits direct access to data in respect of persons under 18 to Europol officials for the performance of their tasks;
- Article 30 (5) restricts the further sharing of personal data in respect of persons under 18 with MS, Union bodies, third countries or international organisations to cases where such transfer is strictly necessary and proportionate in individual cases;
- Article 38 defines the responsibility in data protection matters of Europol and Member States.

Europol's internal documents

- AWF Manual[74];
- Europol Analysis System Manual (EAS Manual), Draft April 2018[75];
- Opening Decisions of Operational Analysis projects, of 24 November 2017 and 26 July 2018 (Portfolio)[76];
- Roadmap for improving data quality| data protection compliance in Europol's AWF, 25 February 2016 (Roadmap for data protection compliance)[77].

Other relevant documents

- Europol National Unit Handbook for the transmission of personal data to Europol, JSB Handbook providing guidance to national units (ENU's Handbook);
- Letter from the EDPS to Europol of 22 March 2018[78];
- Articles 16 and 40 of the UN Convention of the Rights of the Child (UNCRC)[79];
- Rule 21, UN (1985), Standard minimum rules for the administration of juvenile justice ('The Beijing Rules'), General Assembly resolution 40/33 of 29 November 1985[80];
- Article 3(3) Treaty on European Union (TEU);
- Article 24 of the Charter of Fundamental Rights of the EU (EU Charter);
- Council of Europe Guidelines on child-friendly justice[81].

Europol's internal criteria

Europol's internal criteria are contained in the Introductory Chapter of the Portfolio of Analysis Projects (AP). They specify the requirement to limit the processing of personal data of persons under 18 to what is strictly necessary and proportionate for preventing or combating crimes that falls within Europol's objectives. They build upon existing rules contained in the AWF Manual and the ENU's Handbook.

In order to define these criteria, Europol has taken into consideration two principles of the United Nation Convention for the Rights of the Child (UNCRC):

- States Parties shall seek to establish a minimum age below which persons under 18 should be presumed not to have the capacity to infringe the penal law;
- No person under 18 should be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, or to unlawful attacks on his or her honour or reputation.

Europol distinguishes between the processing of personal data of persons under 18 on the basis of their personal implication:

- ***Persons under 18 labelled as suspects, convicted persons or potential criminals***:
    - The strict necessity of the processing for the purpose of the AP can be elaborated in each individual case if there are substantive grounds for assuming that the data are relevant for the aim of the AP as established in the respective OD.

---

79 http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx

80 http://www.ohchr.org/Documents/ProfessionalInterest/beijingrules.pdf

- The provisions under national law providing that persons under 18 can be sanctioned for the offence in question should be mentioned in the respective free-text field of the database. Specific emphasis is put on persons under 15 as not all MS penalize at that age.

- ***Persons under 18 labelled as associate, contacts, victims, witnesses, informants***:
-
  - There must be a specific justification in the OD of the AP;
  - They can only be processed if linked to specific investigations where they appear as such. This second requirements does however not apply to persons under 18 labelled as "informants".

The draft EAS Manual further requires that in all cases a justification is added to the database entry explaining why the processing is necessary and proportionate.

Persons under 18 as vulnerable group of persons and specific international instruments adopted accordingly

1) Persons under 18 as vulnerable group of people deserving specific protection

Article 30 ER acknowledges persons under 18 as a specific category of data subjects, next to other categories (victims, witnesses, informants), who require specific attention from Europol. Processing of data about persons under 18 shall be allowed only if "it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives".

The recognition of persons under 18 as data subjects in need of specific protection echoes the specific treatment these received in the Treaty of Lisbon and the EU Charter, as well as in international instruments such as the UN Convention on the Rights of the Child (UNCRC). Children are entitled to specific protection because "the child, by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection, before as well as after birth"[82]. Under the UNCRC, children means "every human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier"[83].

The promotion and protection of the rights of the child is one of the objectives of the EU on which the Treaty of Lisbon has put further emphasis.[84] Notably, Article 3(3) TEU explicitly requires the EU to promote the protection of the rights of the child. Article 24 of the EU Charter acknowledges children as independent and autonomous holders of rights. Children now "have the right to such protection and care as is necessary for their well-being". In line with Article 3 UNCRC, the EU Charter also makes the child's best interests a primary consideration for public authorities and private institutions. The concept of the child's best interests aims to ensure both the full and effective enjoyment of all the rights recognized in the UNCRC and the holistic development of the child, i.e. child's physical, mental, spiritual, moral, psychological and social development.[85]

The EC undertook a series of actions to implement this objective. On 15 February 2011, the EC adopted an "An EU agenda for the rights of the child" whose purpose is to reaffirm a strong commitment of all EU institutions and of all MS to promoting, protecting and fulfilling the rights of the child in all relevant EU policies. The EC identifies a series of action items to achieve "making the rights of the child an integral part of the EU's fundamental rights policy", namely: making the justice system more child-friendly, targeting EU action to protect children when they are vulnerable, taking into account children in the EU's external action, child participation and awareness raising. This Communication was followed by a number of legislative proposals.

2) The protection of persons under 18 in the criminal justice system

One action item of the EC is of particular interest for the purpose of this inspection report, namely: "Making the justice system more child-friendly in Europe".[86] The objective of ensuring a "Child-friendly justice" is to preserve children's potential for development and reintegration into society.[87] It is also to ensure a "justice that is accessible, age appropriate, speedy, diligent, adapted to and focused on the needs and rights of the child, respecting the rights of the child including the rights to due process, to participate in and to understand the proceedings, to respect for private and family life and to integrity and dignity"[88]. "Justice" is understood broadly and includes all professionals dealing with children in and outside judicial proceedings. Police is explicitly mentioned as one of the sectors responsible for making justice more child-friendly.[89]

The EC outlines that children may become involved with justice systems in a number of ways, for example when they commit offences, when they witness crimes or are their victims, or when they seek asylum. The main points of vulnerability are identified as follows:

- obstacles with regard to legal representation or to being heard by judges;
- inadequate information necessary for children and their representative to exercise their rights or defend their interests in judicial proceedings;
- being treated as adults without being afforded specific safeguards in accordance with their needs and vulnerability;
- effective access to justice and participation in administrative and court proceedings.

As far as criminal proceedings are concerned, several aspects are given specific attention:

- **Right to a fair trial**. The right to a fair trial for children **implies the protection of their privacy**, the right to be informed about the charges and the proceedings in a way which is adapted to the child's age and maturity, legal assistance and representation. This also includes procedural rights of suspected or accused persons in particular who cannot understand or follow the content or the meaning of the proceedings owing to their age, mental or physical condition.

- **Detention of children**. Children sentenced to custody and placed in criminal detention structures are particularly at risk of violence and maltreatment. Detention of children should be a measure of last resort and for the shortest appropriate period of time.
- **Victims and witnesses**. Children participating as witnesses or victims in criminal judicial proceedings who are exploited in criminal activities, such as trafficking of illicit drugs should be protected. Child victims should receive adequate support leading to their recovery and compensation for the harm inflicted on them.

The EC adopted **two Directives** in that field: a Directive on victim's rights in order to raise the level of protection of vulnerable victims, including children[90] and a Directive on special safeguards for suspects or accused persons in criminal proceedings who are vulnerable, including children[91].

With regard to the **right to fair trial,** international instruments from the UN[92] and the Council of Europe should also be taken into account.

In particular, **Article 40 of the UNCRC** specifies **that children who are alleged as, accused of, or recognized as having infringed the penal law** should be treated in a manner consistent with the promotion of the child's sense of dignity and worth, which reinforces the child's respect for the human rights and fundamental freedoms of others and which takes into account the child's age and the desirability of promoting the child's reintegration and the child's assuming a constructive role in society.

The **"Beijing Rules"** (UN Standard minimum rules for the administration of Juvenile Justice, adopted by resolution 40/33 of 29 November 1985) apply to **juvenile offenders**, i.e. "a child or young person who is alleged to have committed or who has been found to have committed an offence"[93]. They aim at promoting juvenile welfare to the greatest possible extent, which will minimize the necessity of intervention by the juvenile justice system, and in turn, will reduce the harm that may be caused by such intervention"[94]. Principle 4 provides guidelines for contracting parties to define an **appropriate age of criminal responsibility**. If fixed too low or if there is no lower age limit at all, the notion of responsibility would become meaningless. According to the commentary a "modern approach would be to consider whether a child can live up to the moral and psychological components of criminal responsibility; that is, whether a child, by virtue of her or his individual discernment and understanding, can be held responsible for essentially antisocial behavior". They recall that while such age differs owing to history and culture, in general there is a close relationship between the notion of

responsibility for delinquent or criminal behavior and other social rights and responsibilities (such as marital status, civil majority, etc.)[95].

The **Council of Europe** has also adopted **Guidelines on child-friendly justice**.[96] The guidelines were adopted specifically to ensure that justice is always friendly towards children, no matter who they are or what they have done. This means that the justice system should treat children well, trust them and can be trusted, listen to children and is listened by them, understands children and is understood by them. It is also a system which tells them when they are in the wrong and stands by them to help them find a solution.[97]

These guidelines restate the application of the rule of law principles to children. It also recalls that elements of due process such as the principles of legality and proportionality, the presumption of innocence, the right to a fair trial, the right to legal advice should be guaranteed as they are for adults and should not be minimized or denied under the pretext of the child's best interest.[98] It also restates the right to privacy and personal data of children who are or have been involved in judicial or non-judicial proceedings and other interventions which should be protected in accordance with national law.[99]

The Guidelines finally mandates police to "respect the personal rights and dignity of all children and have regard to their vulnerability, that is, take account of their age and maturity and any special needs of those who may be under a physical or mental disability or have communication difficulties"[100].

3) The right to privacy and data protection of children in the context of criminal justice

The **Beijing Rules**[101] state that juvenile's right to privacy shall be respected at all stages in order to avoid harm being caused to her or him by **undue publicity** or by the **process of labelling**. This rule is grounded on the fact that young persons are **particularly susceptible to stigmatization**. The commentary of the rule refers to criminological research into labelling processes, which has provided evidence of the detrimental effects (of different kinds) resulting from the permanent identification of young persons as "delinquent" or "criminal".[102] The UN Guidelines for the prevention of Juvenile Delinquency (the Riyadh Guidelines) also point to the risks of "labelling young children as 'deviant' or 'delinquent' or 'pre-delinquent'", as it often contributes to the development of a consistent pattern of undesirable behavior by young people.

Records of juvenile offenders should be kept strictly confidential and closed to third parties, and should not be used in adult proceedings in subsequent cases involving the same offender. In its Recommendation on the Criminal Record and Rehabilitation of Convicted Persons, the Council of Europe's Committee of Ministers advised MS to "restrict to the utmost the

communication of decisions relating to minors". **Children with a criminal record should be given a realistic opportunity of rehabilitation and social reintegration.** [103]

The **Council of Europe Guidelines on child-friendly justice**[104] makes an explicit reference to the safeguards that should apply to the processing of personal data of persons under 18. Para. 8 stipulates that "MS should stipulate limited age to all records or documents containing personal and sensitive data of children, in particular in proceedings involving them. If the transfer of personal and sensitive data is necessary, while taking into account the best interest of the child, MS should regulate this transfer in line with relevant data protection legislation." In that respect, the Explanatory memorandum makes an explicit reference to Council of Europe Convention 108[105] and reminds that "children enjoy all rights under this convention even though it does not explicitly refer to children's rights"[106].

At EU level, Article 14 (1) of **Directive on special safeguards for suspects or accused persons in criminal proceedings who are vulnerable, including children**, makes an obligation for MS to ensure that the privacy of the children during criminal proceedings is protected. This article however only refers to aspects such as audiovisual recording of the questioning or the hearing.

Directive (EU) 2016/680 (the "Law Enforcement Directive")[107] refers to "children" as being vulnerable persons and thus worth of specific protection in Recitals 39 and 50. The competent authorities acting as data controllers should adapt the information provided to children to their needs (Recital 39). They should also pay specific attention to the risks posed by the processing of their personal data and to draw up and implement specific safeguards in that respect (Recitals 50 and 51). The Law Enforcement Directive does however not refer to persons under 18 as being a specific category of data subjects which should be distinguished from other categories of data subjects in the system. Article 6 only requires controllers to make a clear distinction between personal data of suspects, convicted, victims and witnesses.

The **Europol Regulation** (Article 30 ER) thus implements a stricter regime than the one set up in the Law Enforcement Directive by requiring Europol to limit the processing of personal data on persons under 18 (including transfers to third parties) to what is strictly necessary and proportionate. Article 31(5) further imposes an obligation for Europol to inform the EDPS on the processing of personal data about persons under 18 for a period exceeding five years.

The concepts of necessity and proportionality

The principle of necessity and proportionality are key principles guiding the interpretation of legitimate derogations to fundamental rights recognized by the EU Charter, such as the rights to data protection (Article 7) and to privacy (Article 8). Article 52 of the EU Charter states that

"subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."

In EU law, necessity and proportionality are linked under the overarching concept of proportionality in the broad sense. The test is made of three aspects: (1) the suitability of the measure, (2) the effectivity of the measure and (3) the proportionality of the measure *stricto sensu*. [108] The first two aspects are assessed under the principle of necessity, while the third one constitutes the proportionality test, in a narrow sense.

The necessity of a measure is thus assessed on the basis of whether:

- The measure is suitable (or appropriate) to achieve its aim (1), i.e. there is a logical link between the measure and the (legitimate) aim pursued. As far as the processing of data on persons under 18 is concerned, the processing of their data should be able to contribute to the prevention and fight against the crimes for which Europol is competent
- The measure constitutes the least restrictive effective means (2), i.e. it is not possible to efficiently prevent and combat the crime at stake without processing personal data of persons under 18.

Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal.[109] The necessity of a measure must be considered in the light of the specific circumstances surrounding the case as well as the provisions of the measure and the concrete purpose it aims to achieve.

In the field of law enforcement, necessity will stem from the prevention of a real danger or the prevention, investigation and prosecution of a specific criminal offence.[110] The fulfilment of these main police tasks requires an evident and direct correlation between the data processing carried out by the police and a situation where persons under 18 have already committed or are likely to commit a crime.[111]

The third test, the assessment of proportionality of the measure (3), aims to make sure that the advantages resulting from the measure are not outweighed by the disadvantages the measure causes with respect to the exercise of the fundamental rights (the impact the processing may have on the individual). In other words, the measure must be reasonable, considering the competing interests of different groups at hand (preventing and combatting serious crime v. the protection of persons under 18). The specific vulnerability of persons under 18 and the

requirement to act in their best interests, as elaborated in the section above, should be taken into account in the assessment.

It follows from this brief analysis that the assessment of the necessity and proportionality of the processing of personal data about persons under 18 is a highly contextual task and cannot be done *in abstracto*.

4.3.3. Actions and findings

4.4. AP Travellers

4.4.1. Background

Purpose of AP Travellers

AP Travellers support law enforcement efforts in preventing or combating terrorism by sharing data analysis on **FTF,** i.e. individuals who travel to terrorist hotspots (i.e. conflict zones and training venues). It focusses on individuals suspected of travelling across international borders to engage in terrorist activities i.e. Syria or Iraq, who may pose a threat to the security of the MS when they return to the EU.

The **threat** posed by these individuals must be **assessed on a case by case basis by the MS,** according to the factual and reliable information regarding their suspicious activities before initiating their journey; their links to terrorist or radical networks and individuals; or any other relevant factual information and intelligence. Therefore, the AP shall **not process bulk data**

coming from Passenger Name Record and Advanced Passenger Information systems, if they have not been previously assessed and handled by MS.

AP Travellers also include information on the relevant networks and individuals involved in the **recruitment and** the **trip facilitation** of suspected travellers mentioned before.

Issues with the new EAS (Palantir)

During previous supervisory activities[166], EDPS highlighted issues with Palantir, the new EAS for processing data of several APs, including AP Travellers[167]. Indeed, unlike the other EAS used by Europol ( ), Palantir does not have any mandatory fields. Analysts are thus not obliged to indicate a **personal implication** when they insert data about a data subject into the new EAS[168].

These issues were tackled during the EDPS inspection of December 2017 and reflected in Recommendations of the subsequent inspection report. During this inspection, we nevertheless paid particular attention to issues raised by Palantir (i.e. personal implication) while inspecting AP Travellers.

4.4.2. Criteria

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

- Art. 17(2): processing of personal data retrieved from publicly available sources;
- Art. 17(3): access to data from Union, international or national information systems;
- Art. 18(3) and (4): Processing for the purpose of operational analysis;
- Art. 24 and 25: Transfers of data to EUIs, third countries and international organisations;
- Art. 28: Data protection principles;
- Art. 29: Assessment of reliability of the source and accuracy of the info;
- Art. 30: Processing of special categories of data and of special categories of data subjects.

EDPS also took into consideration the following Europol's main internal documents:

- Portfolio of the operational analysis projects (as updated on 27/7/2018)[174];
- Briefing note. Road map for improving data quality[175];
- Management Board Decision adopting the guidelines further specifying the procedures for processing of information for the European Law Enforcement Agency in accordance with Article 18(6) and (7) ER (IDMC Guidelines)[176];
- Analysis Work File Manual[177];
- Draft EAS Manual[178].

4.4.3. Actions and findings

175 EDOC#819460.

176 EDOC #832396 v36A. These guidelines were adopted by the Management Board of Europol on 13 December 2017.

177 EDOC#660518v11.

178 EDOC #886249.

4.5. Palantir Gotham (technical)

4.5.1. Background

The Europol Analysis System (EAS) is Europol's main operational IT system.
EAS version 3.0 is built on top of a product named Palantir Gotham. As it is a complex IT system, the migration started in 2017 but continued during 2018.

The EDPS May 2018 inspection report includes findings related to **severe ER compliance issues** on EAS version 3.0 and a list of recommendations to address them.

List of recommendations in the EDPS May 2018 inspection report specific to EAS 3.0	
	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.
	Ensure that Palantir allows the insertion of the data subject with the **personal implication** for which this person has to be included **in each AP** (so that the person correctly appears, for example, as 'witness' in AP alfa, and as 'suspect' in AP beta).
	Ensure that Palantir allows for the prompt availability of **statistics** on the insertion of **minors** for each and every AP. Given the extremely vulnerable position of minors **below 15**, ensure that Palantir, as is the case with the current iBase system, provide the possibility to receive statistics and to promptly retrieve/single out (for further checks by the DPF and the Supervisory authorities) all cases of minors, below 18 and below 15 years old.
	Revise Palantir's data model to include **mandatory fields for special categories of personal data** where (and only where) such personal data (if allowed by the OD of the AP) can be inserted.
	Revise the ontology of Palantir to ensure Europol's capability to comply with the obligation for Europol to provide the EDPS the **statistics referred to under Article 30(6) ER and information referred to in Article 31(3) ER**.

Early in 2018, Europol informed the EDPS of performance issues that forced to stop the migration process halfway.

4.5.2. Criteria

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 28 on general data protection principles;
- Article 32 on security of processing;
- Article 33 on data protection by design

The following **Europol's internal documents** were also considered:

4.5.3. Actions and findings

During the on-site activities, the inspection team (team C) met the EAS Business Product Manager and employees of ICT Planning & Execution Coordination unit, ICT Solution Architecture & Engineering Coordination unit, the Application Delivery Services unit, Application Delivery Services, Commecial Law unit and DPF.

The interviews were followed by hands-on demonstrations.

All inspection activities are described in detail in the inspection minutes.[210] This section focuses on the most relevant inspection activities and in particular on activities which triggered findings and recommendations.

EAS 3.0 procurement

The aim of this part of the inspection was to understand why Palantir was selected for the new EAS and the impact of data protection features and risks in the selection.

This selection is the result of a **tender procedure** that started in 2012.

The procurement procedure started from an **assessment of the business needs** to be included in the tender. This assessment was done by business analysts and ICT staff and end up with a list of requirements that were labelled as desirable or mandatory.

In the first stage, 74 companies requested the documents and expressed interest in the tender while only 19 actually presented **pre-qualification** questionnaires. The applicants could qualify for the second phase of the procurement procedure based on the assessment of the information provided when confronted with the exclusion and selection criteria[211]. The exclusion criteria were related to economic and financial capacity, and legal capacity. The selection criteria related to the 'technical and professional capacity' used to prove that applicants have sufficient technical and professional capacity to perform the contract. The selection criteria took into account topics like knowledge transfer, staffing capacity and previous projects of similar characteristics. The selection criteria on this first phase did not include any criteria related to data protection (e.g. serious security or personal data breaches).

The evaluation committee recommended to request an offer to the companies with 5 top scores. Only 2 of the 5 companies sent offers to Europol. On 20 July 2012 the **tender** was **canceled** as one company rejected Europol's terms and conditions and the other's solution was uncompliant with the technical requirements as it was not based on Microsoft Windows technology. The procurement was relaunched again allowing non-Windows based solutions. Once again only two companies presented offers and one of them rejected Europol's terms and conditions leaving the other one alone in the tender.

The winner of the procurement procedure was **Capgemini**, who presented a project with **Palantir Technologies Inc. as subcontractor**. The winner project proposed to build the new EAS customizing an analysis tool named Palantir Gotham (Palantir). The latter is comprised of a core package and a set of optional modules that add different functionalities to the system.

EAS 3.0 development

In the initial phase of the project, Capgemini was in charge of **customizing Palantir** to the business needs of Europol and Europol was responsible for integrating Palantir with the other Europol developed IT systems.

The quality of the software developed by the contractor never met Europol's requirement. Europol lost its confidence in the contractor and in 2016 Europol decided to **reboot the project**. Europol analysed the status of each component of the project and decided which ones were properly developed, which could be fixed to meet the requirements and which should be discarded.

After a first 'core Implementation', an **incremental approach** has been followed over the years, in which every time Europol implemented some of the requirements with the assistance of Palantir Technologies Inc. when needed. In this process, that has been repeated several times, users have been performing smoke tests (software tests aimed to check if the critical functionalities are properly working). Additionally users completed an acceptance test for the CT and SOC migration scripts. However, users have not been involved in normal testing cycles. This testing step can take some time depending on the complexity of the newly implemented functionality, normally in the order of two-three weeks.

Europol has a specific unit that takes care of drafting the requirements for any IT system, but the DPF was involved in the project and participated in the drafting of the system requirements included in the call for tenders.

As part of the offer, the **tender specifications**[212] required the tenderers to fill a **compliance matrix**. This document includes EAS 302 initial requirements. For each requirement, applicants must specify if it was covered by the offer and how. 61 of the initial requirements are categorized as "Security & Data Protection" and of those 12 are labeled as mandatory. The requirements descriptions in the compliance matrix are general. An example could be the following: "Personal data (e.g. submitted through forms, kept in logs, etc.) can be removed from the solution at the end of its retention periods, which can be administratively defined. This included user information contained in log files."

The compliance matrix filled by the winner of the tender[213] stated that their offer covered all but 4 of the "Security & Data Protection" requirements. None of the missing requirements in the offer were mandatory.

The inspection team accessed TopTeam, the tool used during EAS 3.0 development to document the requirements. In response to the inspection team request, on 23 May 2018 Europol drafted and provided a report named 'Security and Data Protection Requirements'[214]. Each requirement in TopTeam contains two identifiers, the status and category of the requirement, and a description that is generally associated to EAS business logic. The description level of detail is very different from one requirement to another. Some requirements, like RQ-19837, do not have any description at all, others, like RQ-16722, are two lines long and others, like RQ-14226, are one page long.

Even if there are 61 **data protection and security requirements** in the compliance matrix, the development requirements list of EAS 3.0 is composed of 27 items. One of them was removed.

Requirement category	**Status**	
	New	**Done**
Data Protection	13	5
Security	2	5
No category	0	1
TOTAL	**15**	**11**

The requirements labeled as new are not fully implemented by EAS 3.0. According to the report, two years after the roll out of the first version and with a data migration ongoing, EAS 3.0 fully met around 40% of its data protection and security requirements.

During the December 2017 inspection, Europol provided the System Specific Security Requirements for EAS 3.0[215]. According to Europol the security requirements in this document come from the call for tenders while others come from the analysis of the optional modules that were already part of the IT system. The requirements of this report have a different wording than the ones in the report 'Security and Data Protection Requirements'.

Europol has at least three documents that contain data protection and security related requirements for EAS 3.0: the compliance matrix, the list of requirements to be developed in the TopTeam tool and those in the System Specific Security Requirements document. There is no common requirement wording nor easy way to manage the three lists and ensure that the IT system developed fulfills all the three lists.

Europol did not conduct a formal IT security risk assessment for EAS 3.0.

Europol conducted a project risk assessment following PRINCE 2 methodology[216]. The inspection team accessed the tool used to document the project risk assessment and discovered that **on the analysed risks none were related to data protection**. The risk assessment evaluated only the alternatives: do vs. do nothing.

EAS 3.0 deployment

Europol decided to start with the smallest data groups. In December 2016 the first version of the EAS 3.0 was rolled out in with the **migration** of data from data group . In July 2017 data from data group were migrated from EAS 2.0 to EAS 3.0.

The migration of data was planned for Q1 2018. While testing the migration processes and based on user feedback, severe performance issues were found.

After the inspection, Europol provided updated information on the topic. The latest information Europol was provided in the EDOC #984647v17 dated 20 September 2018. The document is addressed to Europol's Management Board and concludes that Palantir technology is not capable of fulfilling Europol's requirements regarding performance or data protection. The document describes future plans for the EAS to evolve to a solution based on a data lake concept.t[219] The document gives a general overview of the target state and the steps forward, but does not include any plans on how or when the data protection issues detected during the last inspection are going to be addressed.

EAS 3.0 data intake and quality

Contributions with personal data to be included in EAS might come from different sources:

- SIENA, the secure messaging system used by Europol and MS to exchange information;
- Large File Exchange (LFE)[220];

- Handover from data carriers (e.g. hard copies or a DVD);
- Data obtained from , a commercial product used to extract (forensic) data from mobile devices, satellite phones and GPS device.

RAPTOR, the Palantir technologies' service that allows for federated searching of external data sources, is not deployed or foreseen to be deployed.

Palantir's ontology is the data model that allows to define what kind of data are stored in EAS and the relations among those data. Three versions of the ontology have been rolled out: December 2016, June 2017 and January 2018.

The structure of any data to be imported into Palantir as an entity is checked against Palantir's ontology and rejected if found non complaint.

4.5.4. Conclusion and recommendations

Europol **involved the DPF** in the early stages of the EAS tender procedure and development, taking advantage of their expertise in data protection.

Data protection requirements were included in the compliance matrix filled by the applicants in the shortlist, but **data protection and security were not part of the selection criteria** in the questionnaire used to assess which of the applicants were the most suited candidates to provide the EAS 3.0. Europol stated that these preconditions are strictly regulated in Council Regulation 1605/2002 (Financial Regulation), but nothing in the Regulation prevents Europol from including data protection as part of the selection criteria.

The compliance matrix data protection and security requirements were not adequately translated to development requirements. The **follow up of the development requirements** has failed and raises a serious issue: two years after the roll out of the first EAS 3.0 version more than half of the existing data protection development requirements are not implemented.

The **EAS 3.0 users** were involved in the drafting of the requirements but were **not entirely involved in normal testing cycles**. Having the users involved in the testing at earlier stages

would allow Europol to design and conduct better and more meaningful tests for their IT systems.

The **risk analysis** carried out in the procurement process of EAS 3.0 is a strategic risk and did not take into account data protection related risks. No formal security risk assessment[230] or data protection impact assessment[231] were conducted during the lifecycle of EAS 3.0.

The inspection team found very satisfactory the **security measures** in place to prevent that data exported from EAS 3.0 is leaked.

The documents describing the **user roles** in the EAS are not fully consistent with the documented requirements on access control. The documents lack descriptions or use cases that would allow understanding if the allocated permissions cover or not the needs of a given role.

The **recommendations included in the EDPS May 2018 inspection report** were not implemented by the time the 2018 inspection was conducted, since Europol received them only a few days earlier. However, most of the findings related to the EAS 3.0 were well known to Europol since late December 2017. By the time the 2018 inspection was concluded, there was no planning for the required changes.

It is necessary that Europol drafts a clear plan with a defined timeline that will solve the detected incompliances with the Europol Regulation. If a new IT system is going to replace EAS 3.0, Europol must ensure its compliance with the data protection requirements of the Europol Regulation.

The recommendations included in this and the previous report are independent of the technical solutions adopted by Europol, and should be followed on the current IT system as well as on whichever system replaces it.

Therefore, the EDPS makes the following recommendations:

No.	Content
	Include **data protection related criteria** in the pre-selection phase of any procurement processes of IT systems processing personal data.

No.	Content
	Involve the users of IT systems in general, and EAS in particular, in the **testing lifecycle**.
	Ensure that uniform **data quality checks** are carried out in all EAS personal data, regardless of its origin or the user's decisions.
	Prioritize the development of solutions to **address the ER incompliances** detected during the December 2017 inspection (cf. Recommendations of the EDPS May 2018 inspection report).
	Review and update the **user roles documentation** to ensure it is in line with the EAS requirements in access control.

5.1. Background

The inspection team (team A) examined the recruitment policy of Europol focusing in particular on data quality aspects, confidentiality and security issues as well as data subjects' access rights.

5.2. Criteria

The inspection team examined selective topics (see below) of the selection process in light of Regulation 45/2001 (now replaced with Regulation 2018/1275), the EDPS Guidelines on recruitment policy[276] and the EDPS Guidelines on the rights of individuals with regard to the processing of personal data[277].

Annex 1 – 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.

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.

...".

Art 58 of Regulation 2018/1725 sets forth the powers of the EDPS as follows:

"...

1. The European Data Protection Supervisor shall have the following investigative powers:

(a) to order the controller and the processor to provide any information it requires for the performance of his or he tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to notify the controller or the processor of an alleged infringement of this Regulation;

(d) to obtain, from the controller ad processor, access to all personal data and to all information necessary for the performance of his or her tasks;

(e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law.

2. The European Data Protection Supervisor shall have the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation;

(c) to refer matters to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;

(d) to order the controller or processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(e) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specific period;

(f) to order the controller to communicate a personal data breach to the data subject;

(g) to impose a temporary or definitive limitation including a ban of processing;

(h) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;

(i) to impose an administrative fine pursuant to Article 66 in the case of non-compliance by a Union institution or body with one of the measures referred to in points (d) to (h) and (j) of this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.

3. *The European Data Protection Supervisor shall have the following authorisation and advisory powers:*

   (a) To advise data subjects in the exercise of their rights; (...)

4. *The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice under the conditions provided for in the Treaties and to intervene in actions brought before the Court of Justice. ...".*

Annex 3 List of abbreviations

AFIS	Automated Fingerprint Identification System
AP	Analysis Project
API	Application Program Interface
AWF	Analysis Work File
BC	Business Continuity
BCF	Business Continuity Framework
BCM	Business Continuity Manager
BPL	Basic Protection Level
BPM	Business Product Manager
CAS	Central Authentication Store
CCTV	Closed Circuit Television
CDBPM	Capabilities Directorate Business Product Management
CFN	Computer Forensic Network
CM	Crisis Management
CMT	Crisis Management Team
CORPNET	Corporate Network
CRI	Common Risk Indicators
CT	Counter Terrorism
CTW	Check the Web
DMZ	Demilitarized Zone
DOB	Date of birth
DPA	Data Protection Authority
DPF	Data Protection Function unit
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EAS	Europol Analysis System
EASO	European Asylum Support Office
EC	European Commission
ECB	Europol Cooperation Board
ECD	Europol Council Decision 2009/371/JHA of 6 April 2009 establishing Europol
ECTC	European Counter-Terrorism Centre
EDOC	Europol Document
EDPS	European Data Protection Supervisor
EIP	Europol Integration Platform
EIS	Europol Information System
ELM	Europol Link Manager
EMSC	European Migrant Smuggling Centre
ENU	Europol National Unit
EPE	Europol Platform for Experts
ER	Regulation 2017/94 (Europol Regulation)
ERES	Enhanced Risk Entities Solution
ETIAS	European Travel Information and Authorisation System
EURTF	European Union Regional Task Force
FTF	Foreign Terrorist Fighter
GO	Guest Officer
HENU	Head of Europol National Unit
IAM	Identity and Access Management
ICE	Immigration and Customs Enforcement (US)
IDMC	Integrated Data Management Concept
IRMa	Internet Referral Management Application
IRU	Internet Referral Unit

IS	Islamic State
JIT	Joint Investigation Team
JSB	Europol Joint Supervisory Body
LEA	Law Enforcement Authority
LFE	Large File Exchange
MACR	Minimum age of criminal responsibility
MER	Main Equipment Room
MS	Member State(s)
NCMEC	National Centre for Missing and Exploited Children
O1	Europol Front Office
OA	Operational Analysis
OCG	Organised Crime Group
OD	Opening Decision
OPSNET	Operational network
OWASP	Open Web Application Security Project
PQL	Palantir Query Language
QUEST	Querying Europol Systems
SER	Secondary Equipment Room
SIEM	Security Information and Event Management
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SNE	Seconded National Experts
SOC	Serious and Organised Crime
SQL	Structured Query Language
SSSR	System Specific Security Requirements
TFTP	Terrorist Financing Tracking Programme
THB	Trafficking of Human Beings
TP	Third Party
UAM	User Account Management
UNCRC	United Nations Convention for the Rights of the Child
UFED	Universal Forensic Extraction Device
USE	Unified Search System
VIS	Visa Information System
VLAN	Virtual Local Area Network