



European Data Protection Supervisor
5th June 2018



Introduction to Palantir



What We Do



COUNTER
TERRORISM



MILITARY



SPECIAL
OPERATIONS



LOCAL LAW
ENFORCEMENT



FINANCE



HEALTHCARE
RESEARCH



AUTOMOTIVE



ENERGY



COUNTER
PROLIFERATION



BANKING



PROSECUTION



AUDIT



RETAIL



PHARMA



TECH



INTELLIGENCE



MEDIA



INSURANCE



HEALTHCARE



DISASTER
RELIEF



CONSUMER
PACKAGED GOODS



CARD
SERVICES



AVIATION

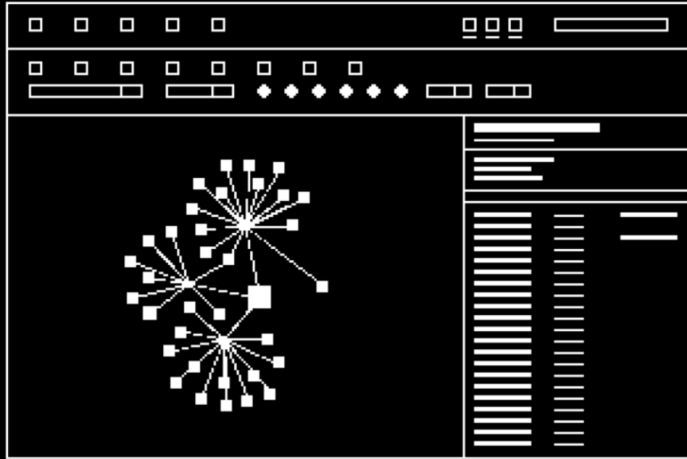


UTILITIES

Design Principles

- Human beings are the best decision-makers, not algorithms
- Data belongs to customers, not to Palantir
- There are no “one-button” solutions for complex challenges
- We do not build systems that undermine fundamental rights

How We Do It



Gotham



Foundry

Privacy and Civil Liberties Engineering



Philosophy of PCL Software Engineering



Everyone is
a PCL Engineer

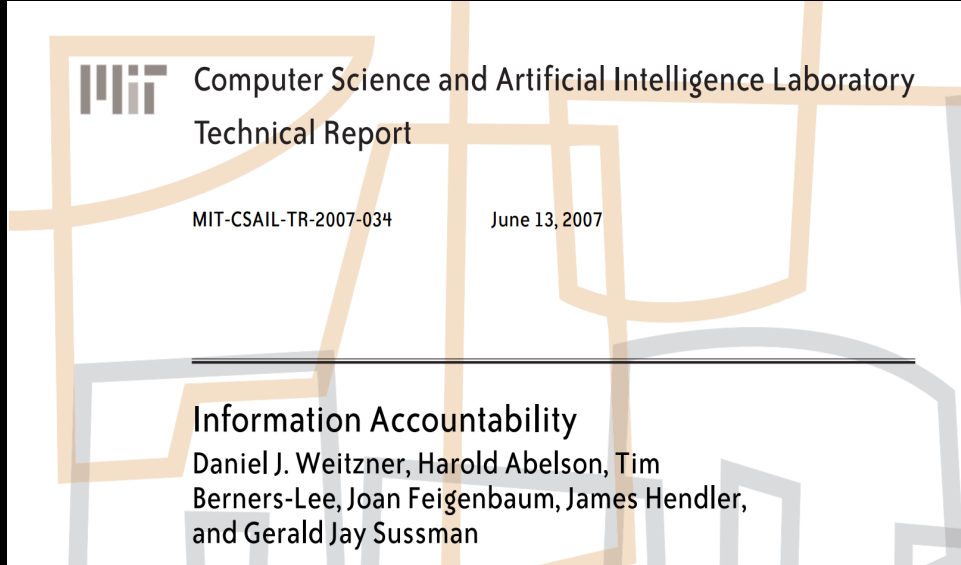


Pro-active
Involvement



Bring Mastery
to Product

Privacy engineering as regulating authorized use



“Debates over online privacy, copyright, and information policy questions have been overly dominated by the access restriction perspective. We propose an alternative to the “hide it or lose it” approach that currently characterizes policy compliance on the Web. Our alternative is to design systems that are oriented toward information accountability and appropriate use, rather than information security and access restriction.”

Metadata Management



Search, navigate, and discover

/Global org/Fraud detection

members

Show advanced

Analyze data

INPUTS

members

[Import](#) • [Edit schema](#)

SUMMARY

Report issue

Enter description...

Updated Sun Sep 10 2017 by kyle_e - Created by kyle_e

/Global org/Fraud detection/members

TAGS

Add tags

TYPE

Raw dataset

DETAILS

1,000 rows · 9 columns

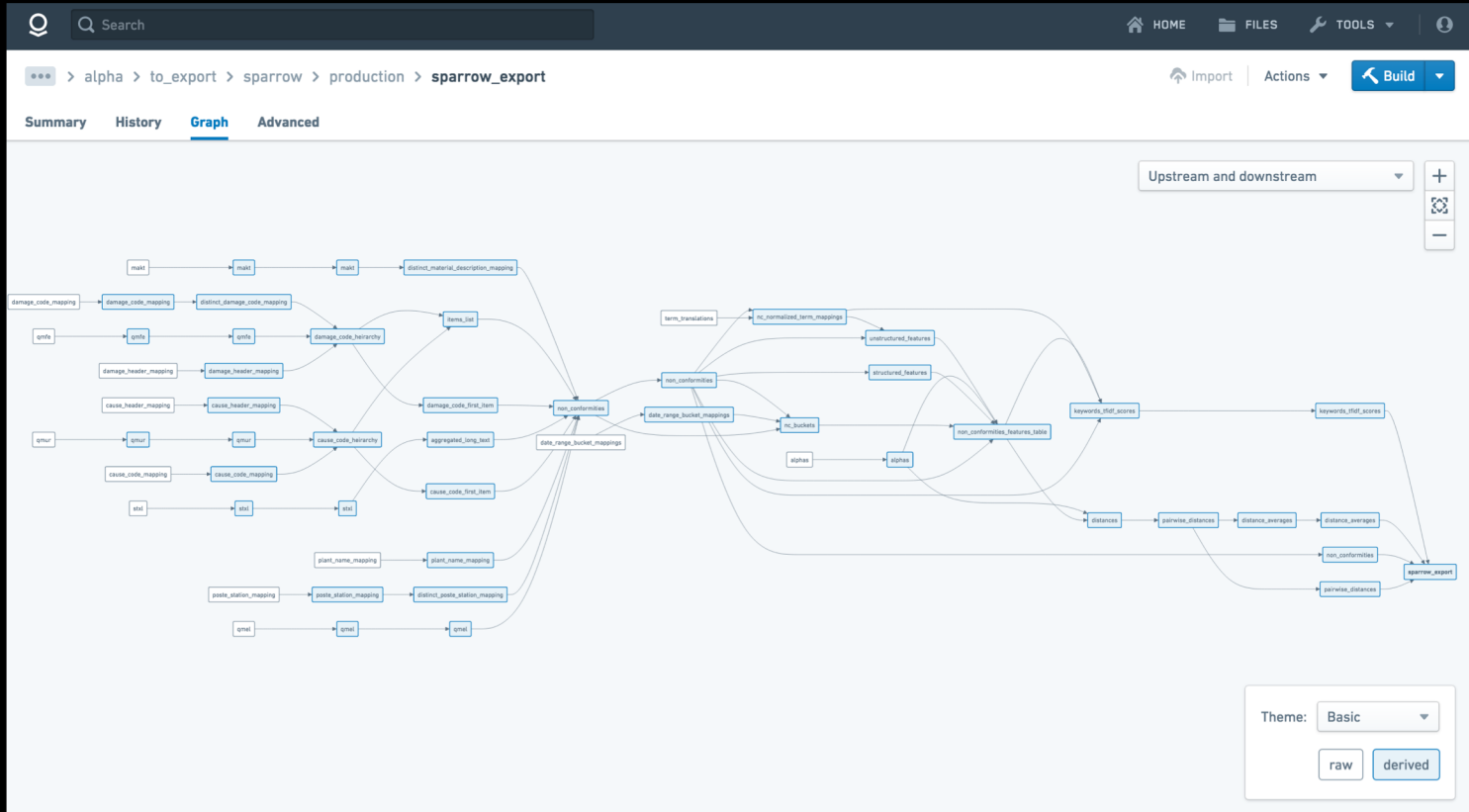
COLUMNS

Filter

	member_id String <input type="text" value="member.id"/>	member_name String <input type="text" value="person.name"/>	gender String <input type="text" value="person.gender"/>	phone_number String <input type="text" value="person.phone"/>	street_address String <input type="text" value="person.address"/>	city String <input type="text" value=""/>	country String <input type="text" value=""/>
1	14-0956579	Emmalee Giddens	Female	1-(303)490-3972	45 Lien Pass	Denver	United States
2	09-1654051	Art Clint	Male	1-(215)174-1038	14482 Schiller Crossing	Philadelphia	United States
3	88-7844528	Kathleen Fosdyke	Male	1-(585)804-2137	14101 Goodland Street	Rochester	United States
4	61-0440231	Wini Davenall	Female	1-(210)959-5334	83 Tony Crossing	San Antonio	United States
5	92-5508391	Neils Gaitskill	Male	1-(602)798-1681	547 Anhalt Trail	Phoenix	United States
6	39-2762050	Raynard Fromant	Male	1-(865)141-3545	679 Moose Center	Knoxville	United States
7	60-5160869	Cicely Maycey	Female	1-(304)336-9877	74 Valley Edge Hill	Charleston	United States
8	39-8435197	Leandra Christofol	Female	1-(314)960-5098	8065 Crowley Junction	Saint Louis	United States
9	08-8161493	Melesa Colbert	Female	1-(205)590-4236	75 Bluestem Pass	Birmingham	United States
10	46-7792128	Raleigh Finlay	Female	1-(704)648-3133	419 Kings Way	Charlotte	United States
11	94-9889797	Marrilee Vicarey	Male	1-(719)968-6054	05030 Golf Junction	Colorado Springs	United States
12	15-5947535	Lindie Geindre	Male	1-(704)802-2982	248 Calypso Plaza	Charlotte	United States
13	61-9216626	Meade Frear	Male	1-(512)632-6822	3166 Butternut Parkway	Austin	United States
14	22-4494607	Brett Bonett	Male	1-(763)463-2378	1791 Arapahoe Pass	Monticello	United States
15	70-5901514	Dalston Ellingsworth	Male	1-(508)672-5647	622 Forest Point	New Bedford	United States
16	86-9783296	Claudelle Sendall	Female	1-(816)201-9907	8441 Mayer Lane	Kansas City	United States
17	16-5145330	Peadar Tissington	Female	1-(717)508-7236	870 Ramsey Center	Lancaster	United States
18	77-0741476	Henderson Hackworth	Female	1-(210)427-1049	1 Bultman Pass	San Antonio	United States
19	11-2552752	Augustine Buret	Female	1-(303)690-8354	73 International Junction	Littleton	United States
20	83-7520801	Paxon Kilmaster	Male	1-(336)804-1239	5 Upham Way	Greensboro	United States



Data Provenance



Purpose Based Controls

The screenshot displays a web application interface for 'Fokuspunkt Manager'. The main window has a dark header with 'import update publish' and a search bar. Below the header is a toolbar with icons for navigation and editing, and a 'Node Size' control. The main content area shows a 'Fokuspunkt Manager' panel with the following fields:

- Navn:** New Fokuspunkt
- Kategori:** Efterforskning og forebyggelse af strafbare forhold
- POLSAS Sag:** Sag Journalnummer: 123-1234-123-17

Buttons for 'Rediger' (orange) and 'Link til valgte sag' are visible at the bottom of the panel.

A modal dialog box titled 'Rediger Fokuspunkt' is open, containing the following form fields:

- Fokuspunkt Navn:** New Fokuspunkt
- Fokuspunkt Kategori:** Radio buttons for:
 - Efterforskning og forebyggelse af strafbare forhold
 - Beredskabsrelaterede opgaver
 - Grænse- og udlændingekontrol
 - Øvrige
- POLSAS Sag Journalnummer:** Indtast eventuelt et Polsas Journalnummer, hvis det er relevant. The input field contains '123-1231-1231-12'.

Buttons for 'Annuller' and 'Rediger Fokuspunkt' are at the bottom of the dialog.

Granular Data Management

Search or browse your files and data...

All projects | **Medical claims** | Owner | FILES | SETTINGS | TRASH | + New

A project for integrating, cleaning and managing medical claims worldwide.

Name	Last updated	Tags
Germany Medical Claims	7 hours ago	
medical_claims_all	Mon, Feb 19, 2018 at 8:13 PM	
medical_claims_austria	Mon, Feb 19, 2018 at 7:50 PM	
medical_claims_canada	Mon, Feb 19, 2018 at 7:50 PM	
medical_claims_eu	Mon, Feb 19, 2018 at 7:54 PM	
medical_claims_europe	Mon, Feb 19, 2018 at 7:57 PM	
medical_claims_france	Mon, Feb 19, 2018 at 7:50 PM	
medical_claims_n_america	Mon, Feb 19, 2018 at 8:04 PM	

Search or browse your files and data...

All projects | **Medical claims**

This is a private project. You may only have access to some files and actions in this project.

A project for integrating, cleaning and managing medical claims worldwide.

FAVORITES | ALL >

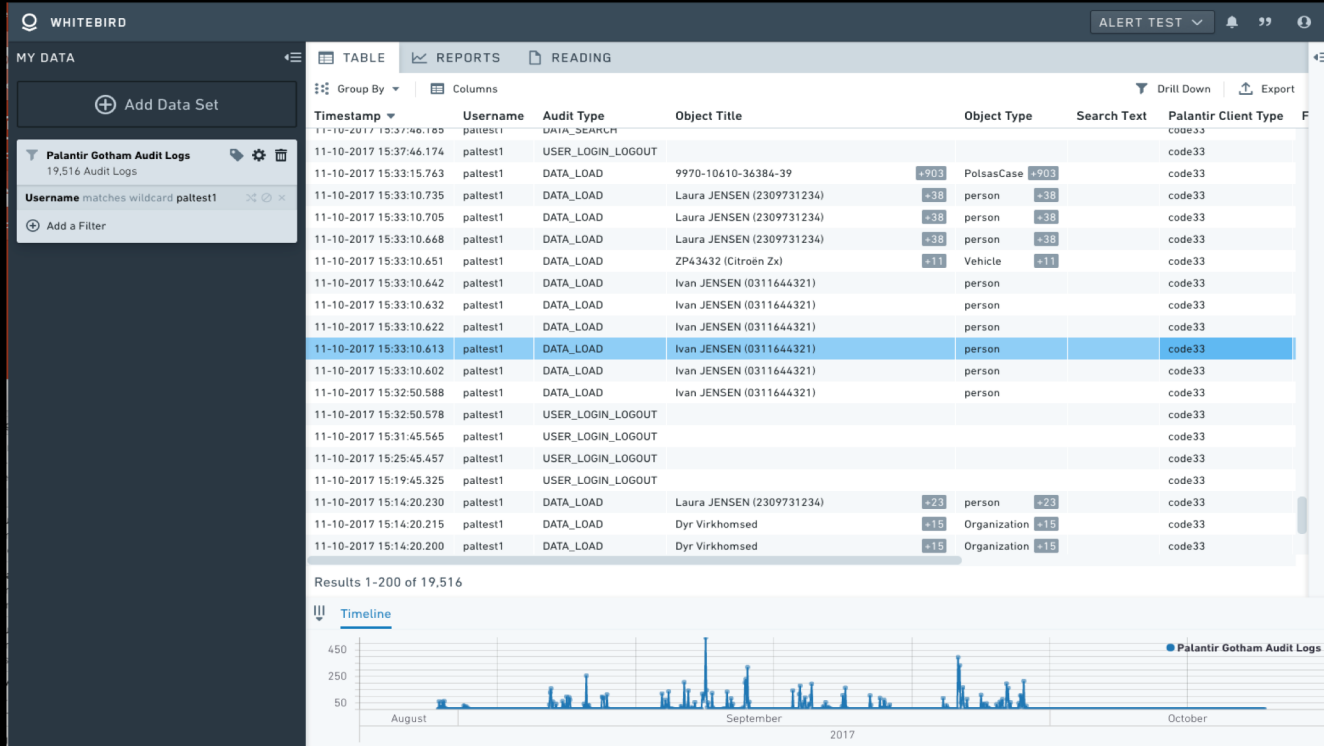
You haven't added any favorites yet

THIS PROJECT IS PRIVATE

You must have access to view or edit it.

[Request access](#)

Auditing Oversight



Retention Management



OBJECTS SCHEDULED FOR DELETION

Filter expiring objects...

Change Object Expirations

	OBJECT NAME	TYPE	NUMBER OF LINKS	NUMBER OF PROPERTIES	DELETION DATE ▼
<input checked="" type="checkbox"/>	Linkage	Gang Affiliation Record	0	2	August 28th, 2015
<input type="checkbox"/>	This person is not a Criminal!	Gang Affiliation Record - Non-Criminal Identifying	2	2	October 27th, 2015
<input type="checkbox"/>	Yet another Gang Affiliation Record	Gang Affiliation Record	5	2	October 30th, 2015
<input checked="" type="checkbox"/>	Linked Gang Affiliation Record	Gang Affiliation Record	1	2	October 30th, 2015
<input checked="" type="checkbox"/>	Not definitively evil	Gang Affiliation Record - Non-Criminal Identifying	1	2	October 30th, 2015
<input checked="" type="checkbox"/>	New Gang Affiliation Record	Gang Affiliation Record	1	2	November 18th, 2015
<input type="checkbox"/>	Another Gang Affiliation Record	Gang Affiliation Record	2	2	November 18th, 2015
<input type="checkbox"/>	Affiliated with bad dudes	Gang Affiliation Record	3	3	November 18th, 2015
<input type="checkbox"/>	Affiliation Record of Evil	Gang Affiliation Record	3	4	April 29th, 2016

← Previous Page

Page 1 of 2

Next Page →



PUTTING IT TOGETHER: FOUNDRY AND THE GDPR



THE STRUGGLE FOR COMPLIANCE

FRAGMENTED
DATA LANDSCAPES



Inability to do basic
accounting of data

PAPER-BASED
COMPLIANCE



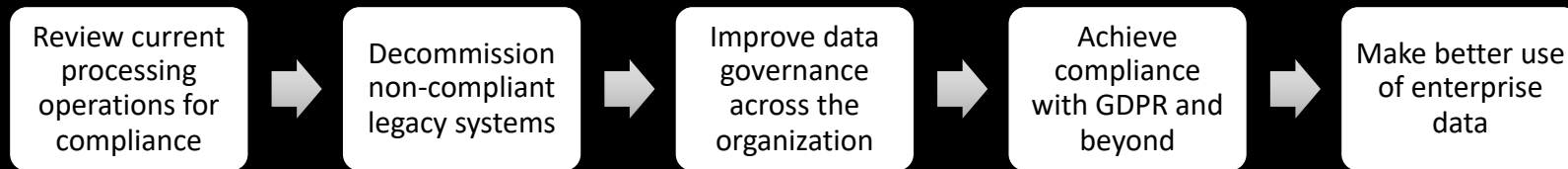
Inefficient and error-
prone procedures

LACK OF CONTEXT-
SPECIFIC GUIDANCE



Uncertainty about what
constitutes compliance

DATA PROTECTION AS AN OPPORTUNITY



FOUNDRY FOR GDPR COMPLIANCE

DATA-DRIVEN ACCOUNTABILITY



Comprehensive overview and control of processing operations

CODE-BASED COMPLIANCE



Rules are dynamically updated and programmatically enforced

INFRASTRUCTURE, NOT A TOOL



Configurable to meet compliance needs of today and tomorrow

FOUNDRY FOR GDPR COMPLIANCE

DISCOVERY / CLASSIFICATION
INTEGRATION / DE-DUPLICATION



Art. 30: Records of processing activities
Art. 35: Data protection impact assessments
Arts. 15-17, 20: Rights to access, rectification, deletion and portability

PROVENANCE / PROCESSING



Art. 5(1)d: Accuracy
Art. 6: Lawfulness of processing
Art. 25: Data protection by design and default

DIFFERENTIATED ACCESS
DYNAMIC DATA MINIMIZATION



Art. 5(1)c: Data minimization
Art. 32: Security of processing

RETENTION / DELETION



Art. 5(1)e: Storage limitation
Art. 17: Right to deletion

AUDITING / OVERSIGHT



Art. 30: Records of processing activities
Art. 5(2): Accountability
Art. 6: Lawfulness of processing

SECURITY



Art. 32: Security of processing



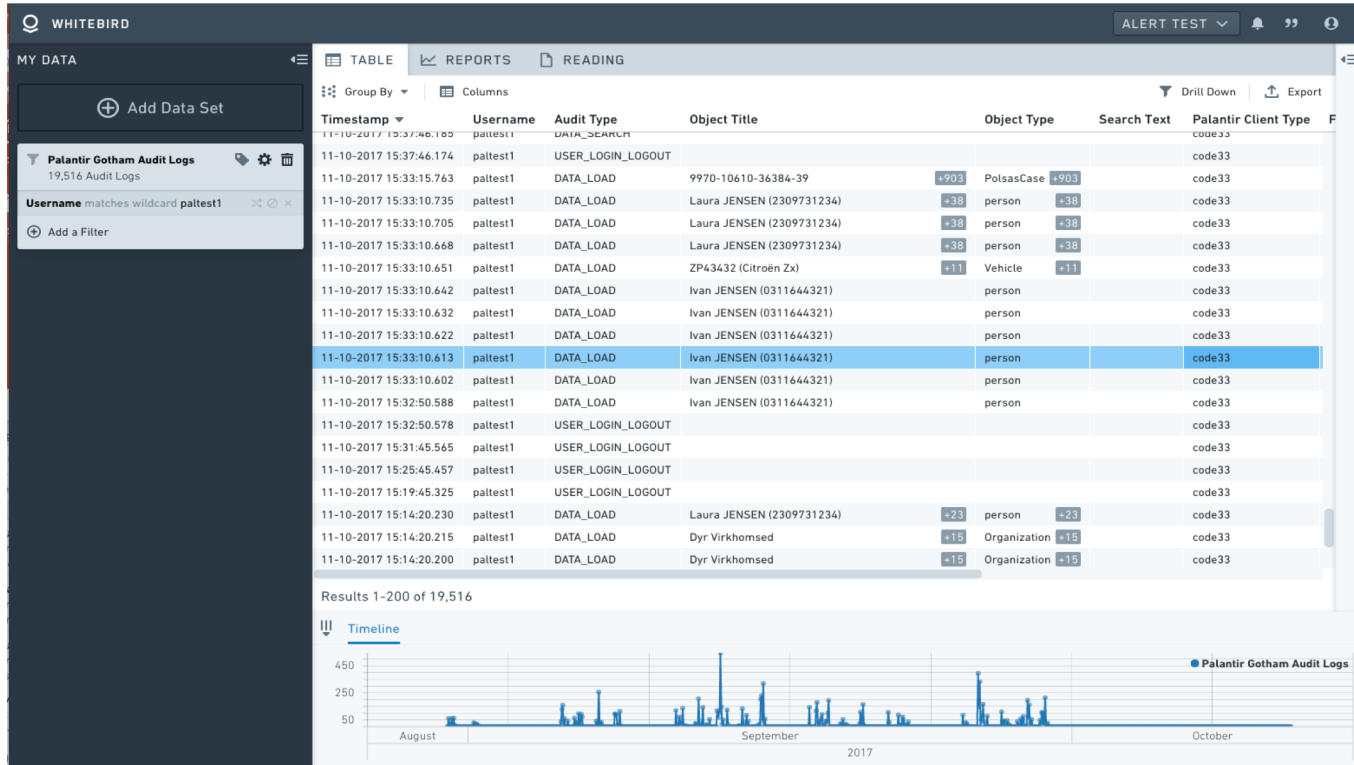
DISCUSSION: TRANSPARENCY THROUGH AUDITING



Sample Audit Log in Standard Universal Format

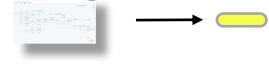
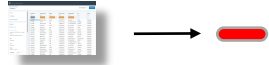
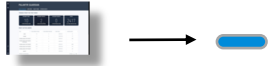
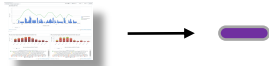
```
<coal:AuditEntry method="Search_search" type="DATA_SEARCH" xmlns:coal="http://www.palantirtech.com/COALSchema_1.14.1" xmlns:sa="http://www.palantirtech.com/SearchAroundTemplate">
  <context sessionId="273295892286969759" remoteAddress="10.5.82.63" clientType="workspace" userId="1"
    instance="POLINTELTEST" trustedSource="true" user="admin" application="pg-server" userName="
    Administrator Account" source="il-pg-alpha-1072800.euw1.palantir.global" sequence="5" timestamp="
    2017-08-31T10:20:20.199+01:00" clientType="workspace" instance="POLINTELTEST" application="
    pg-server"/>
  <entitySets>
    <entitySet totalSize="1" size="1" role="OCCURRED_IN" type="INVESTIGATION">
      <A0Investigation title="rerere|Kriminel" creator="admin" groups="Everyone; idx2_reader;
        pv_reader" id="5965157242781654619"/>
    </entitySet>
    <entitySet totalSize="1" size="1" role="OPERATED_ON" type="SRCH_QUERY">
      <A0Query>
        <operatorType>INTERSECT</operatorType>
        <searchTerms>&lt;untitled Nummerplade&gt;</searchTerms>
        <pageSize>15</pageSize>
        <typeFilters value="[objType = com.palantir.object.entity]" type="SEARCH_FILTER"/>
      </A0Query>
    </entitySet>
    <entitySet totalSize="0" size="0" role="SEARCH_MATCH" type="PTOBJECT"/>
  </entitySets>
</coal:AuditEntry>
```

Audit Log Analysis Application



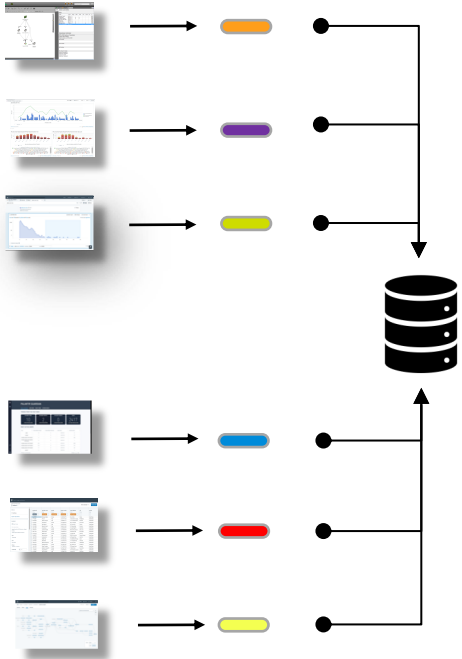
Logs are generated by unique actions and applications

Step 1: Generation



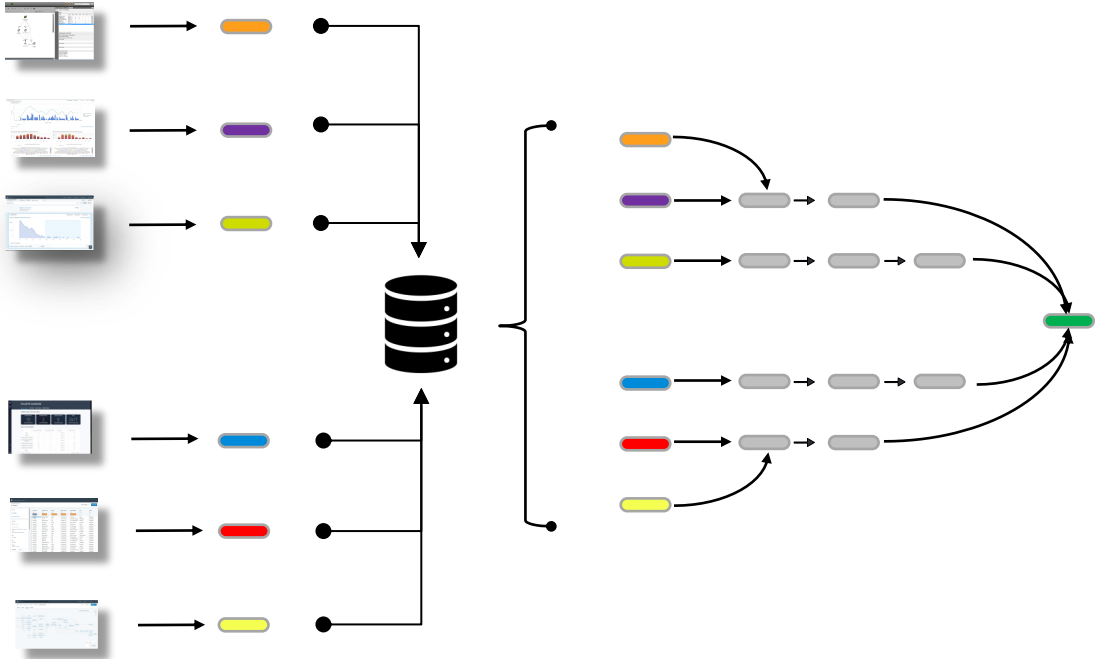
Logs are aggregated into a centralized service

Step 1: Generation Step 2: Aggregation

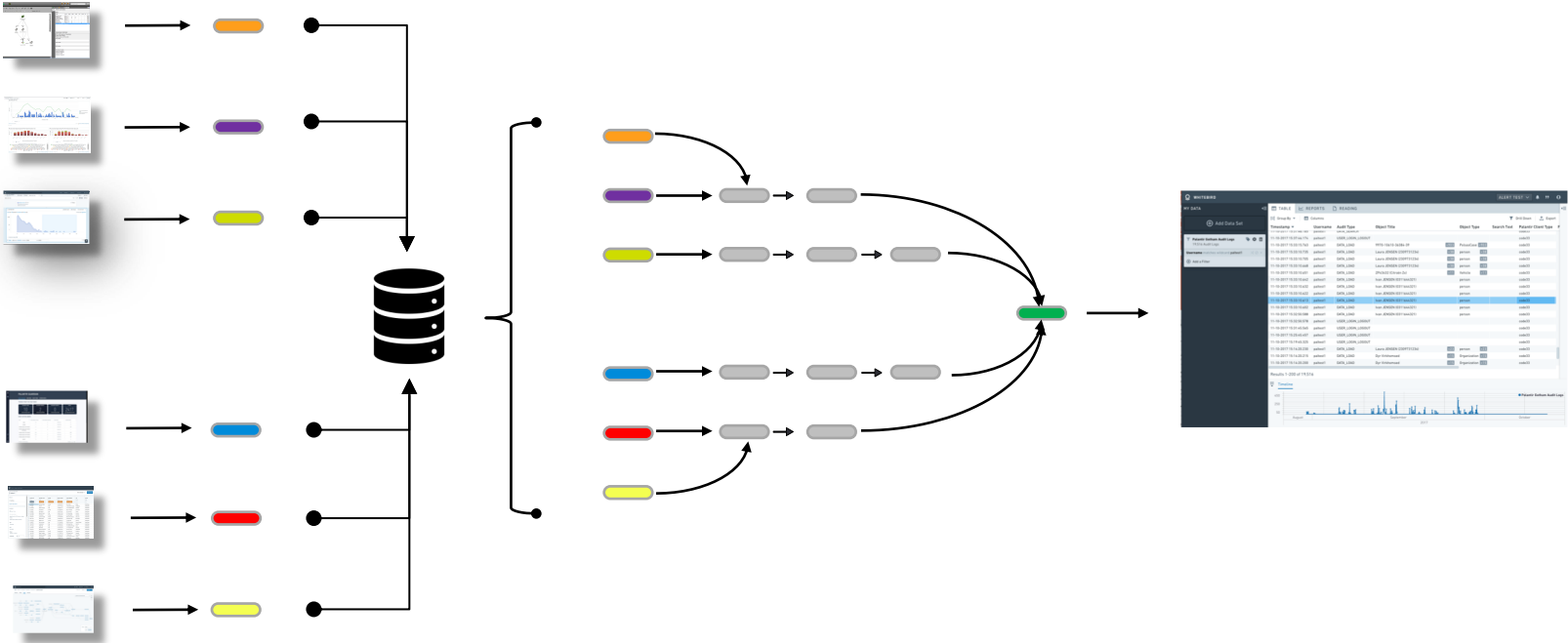


Logs of different formats are integrated into a standardized data format

Step 1: Generation Step 2: Aggregation Step 3: Integration



Standardized log data is ready for analysis



QUESTIONS

- Audit Analysis as System Oversight
- Expectations of Pro-active Auditing
- What would you like to see?

DISCUSSION: TIERED DELETION



DELETION FRAMEWORK



State
Management



Processing
Logic



Orchestration



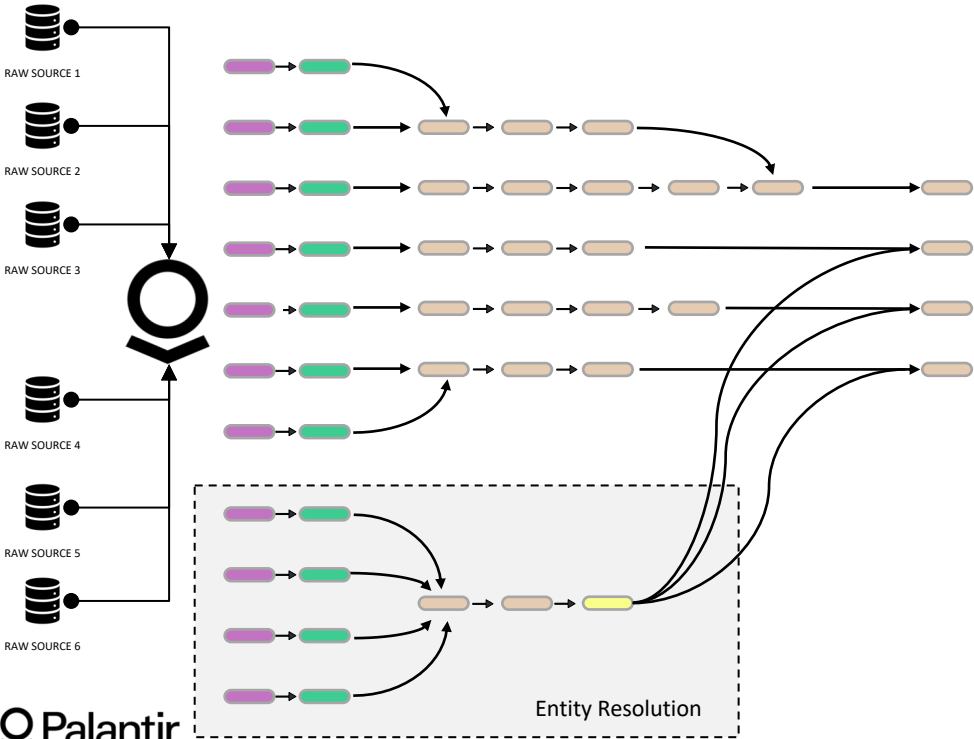
User
Interaction

PALANTIR DATA PIPELINES



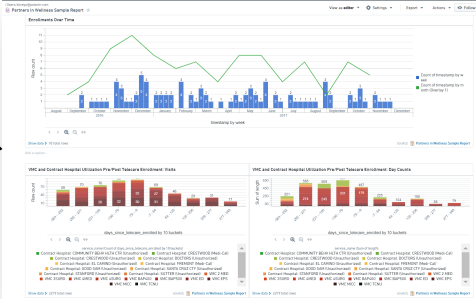
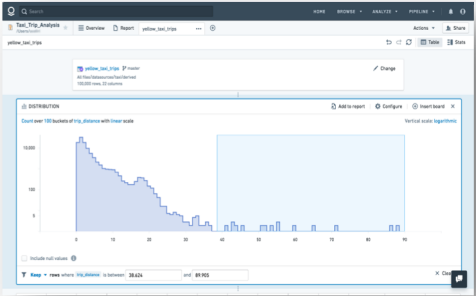
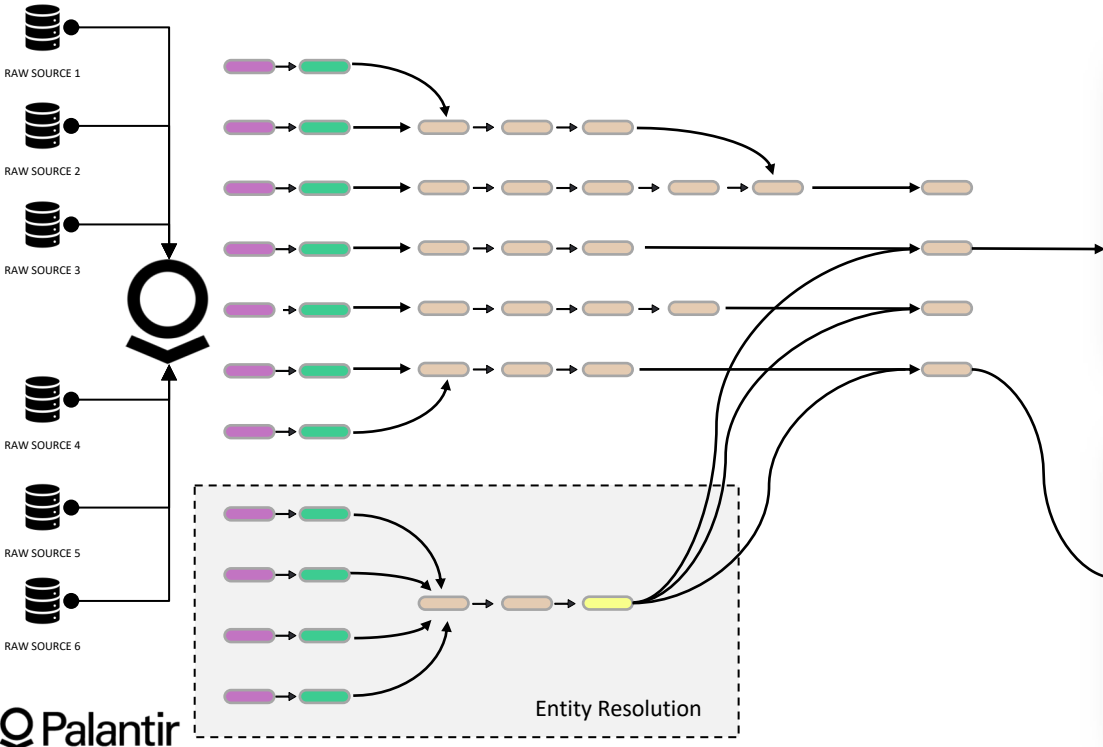
Palantir processes data through pipelines

Step 1: Ingestion Step 2: Cleaning Step 3: Transform



Data that users access run through transformations and checks

Step 1: Ingestion → Step 2: Cleaning → Step 3: Transform → Step 4: Palantir Apps



Secure authentication and access control fences off data in Landing zone from Analysis zone

(ADMIN ONLY ACCESS)  LANDING ZONE

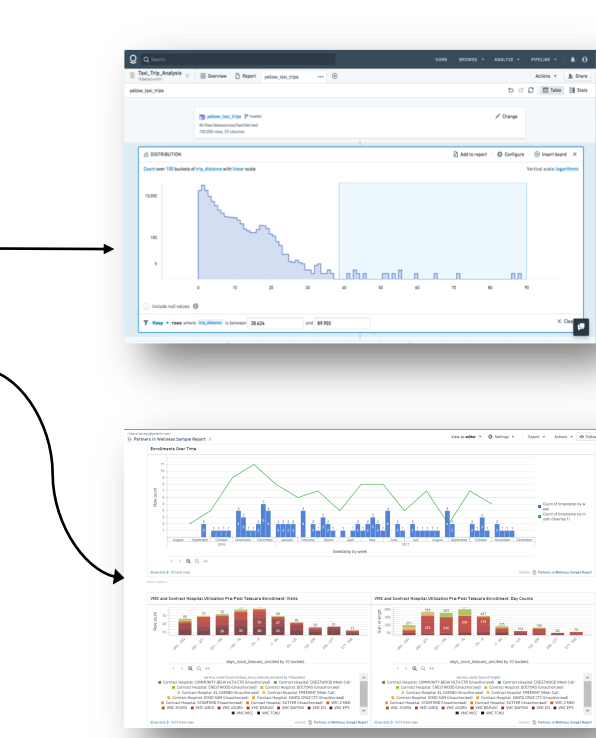
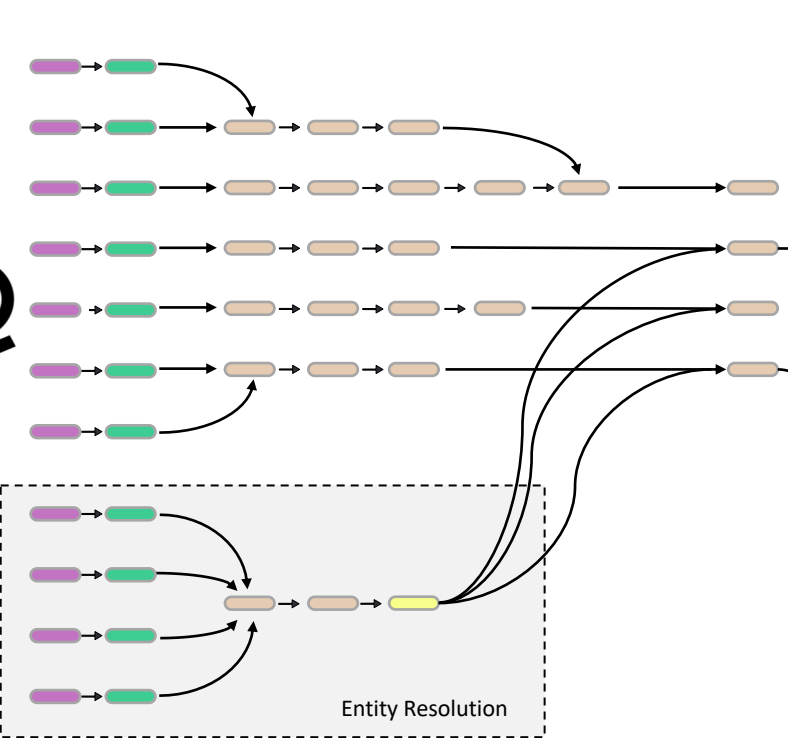
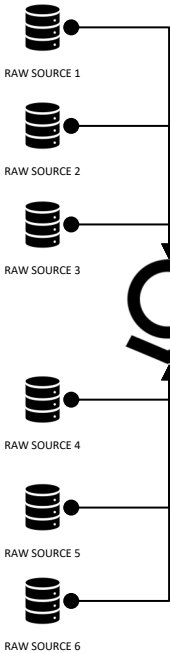
ANALYSIS ZONE  (USER ACCESS)

Step 1: Ingestion

Step 2: Cleaning

Step 3: Transform

Step 4: Palantir Apps



Unauthorized users cannot reach into Landing zone.

(ADMIN ONLY ACCESS)  LANDING ZONE

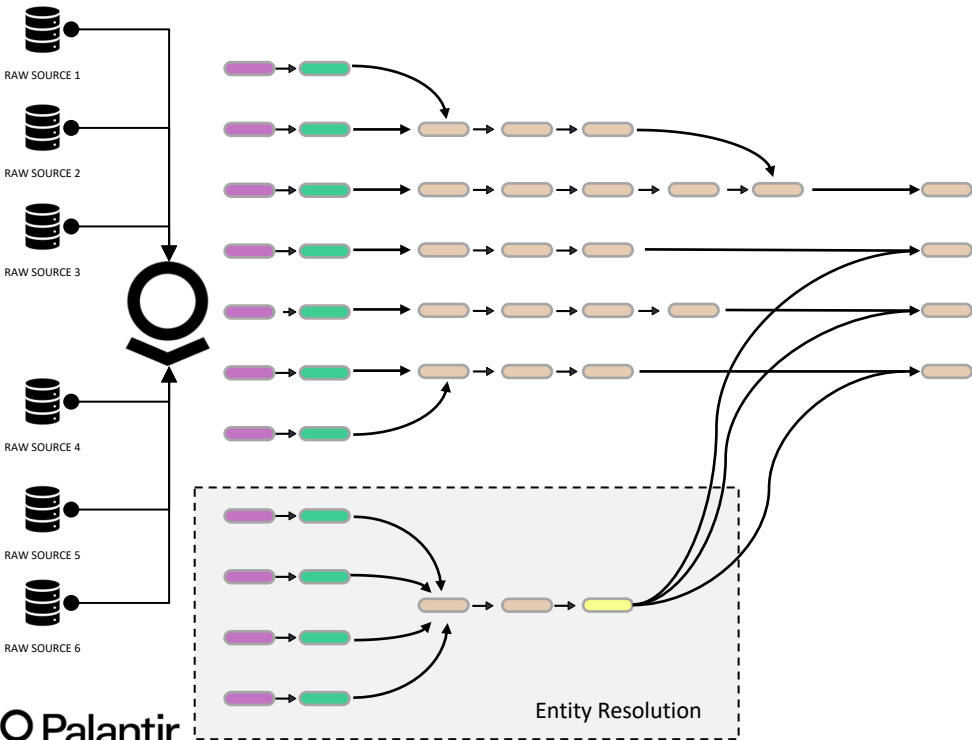
ANALYSIS ZONE  (USER ACCESS)

Step 1: Ingestion

Step 2: Cleaning

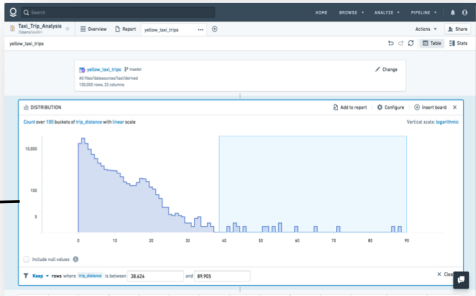
Step 3: Transform

Step 4: Palantir Apps



X

X



DELETION



Past retention date, expired data is removed in Landing zone. Users no longer have access to data.

(ADMIN ONLY ACCESS)  LANDING ZONE

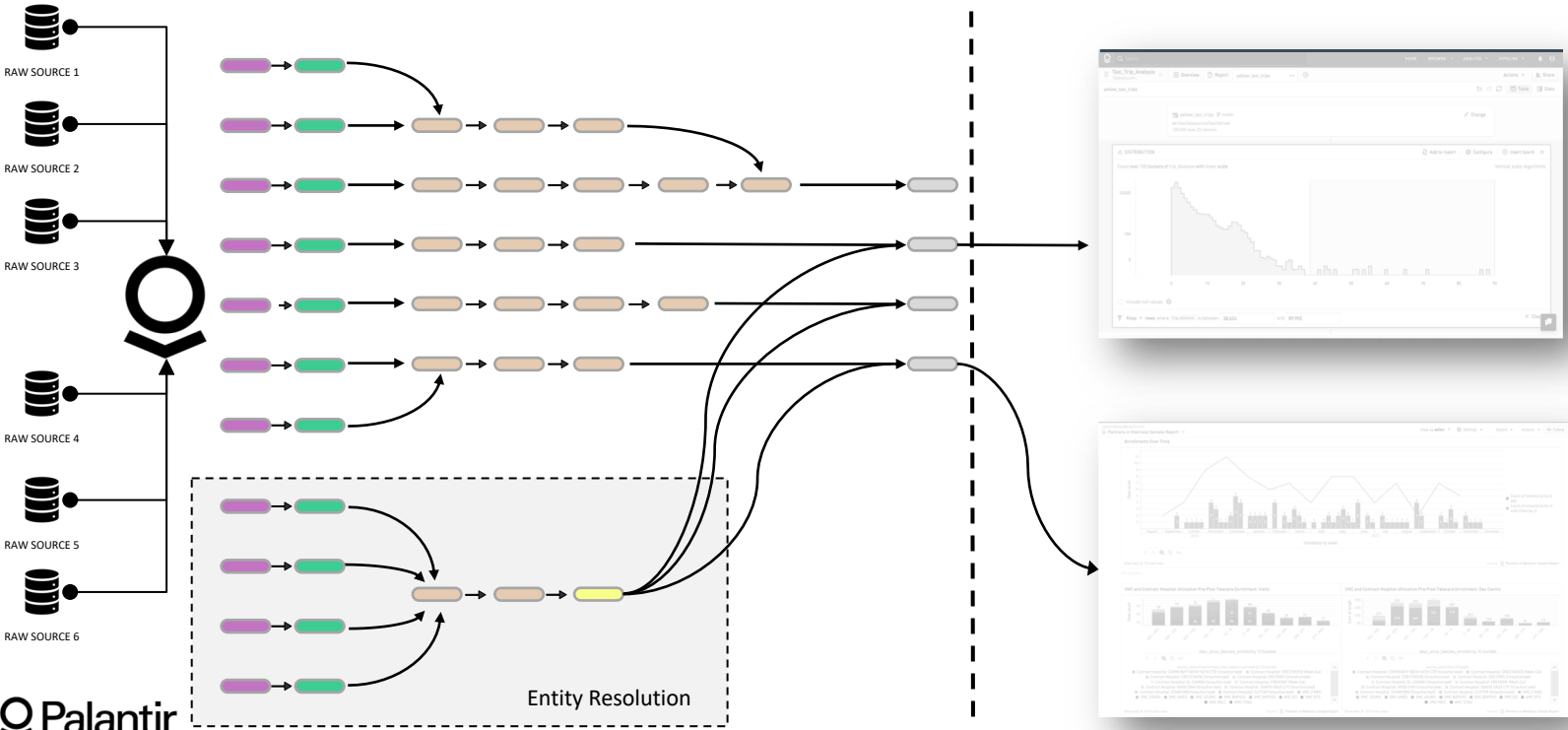
ANALYSIS ZONE  (USER ACCESS)

Step 1: Ingestion

Step 2: Cleaning

Step 3: Transform

Step 4: Palantir Apps



Once source data is removed...

(ADMIN ONLY ACCESS)



LANDING ZONE

ANALYSIS ZONE



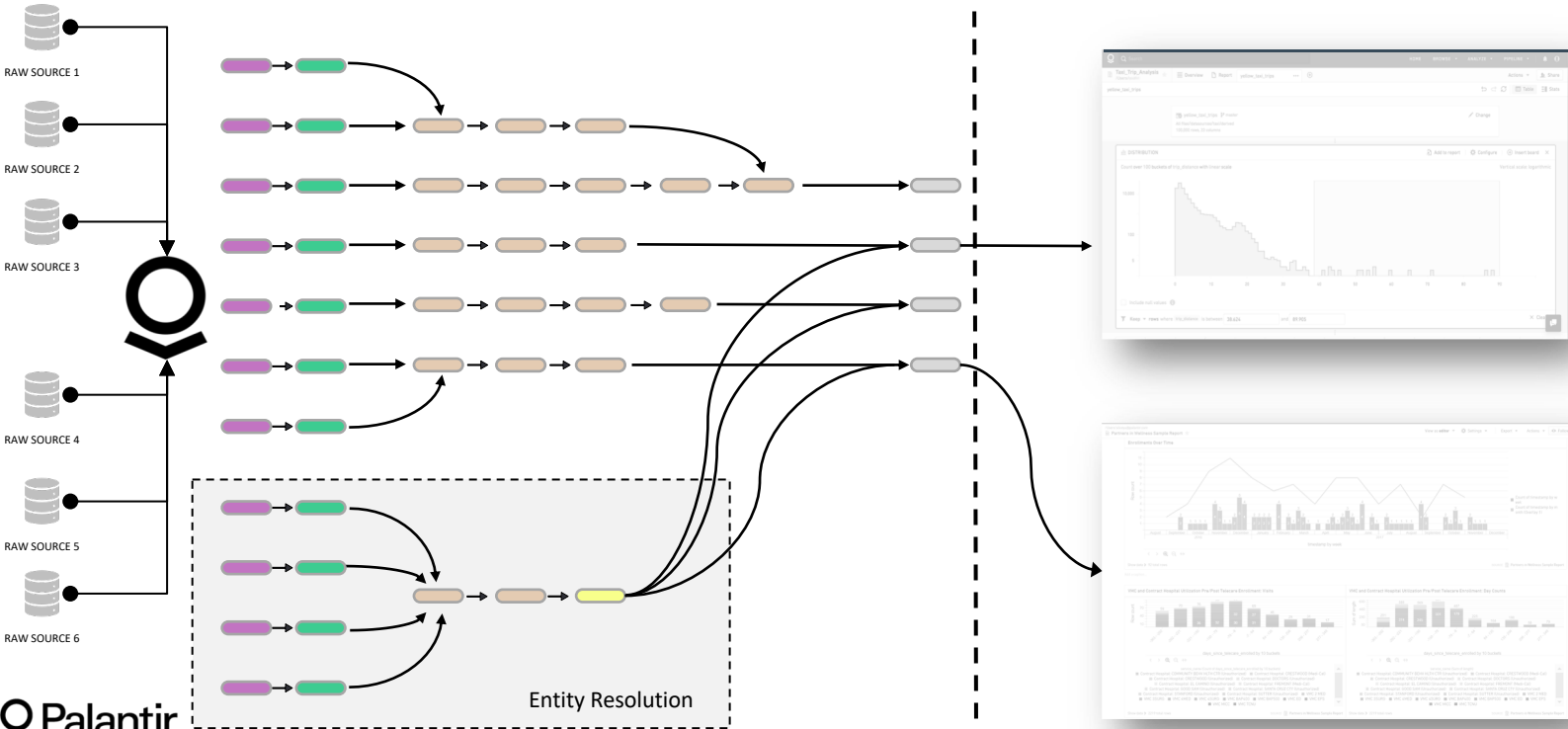
(USER ACCESS)

Step 1: Ingestion

Step 2: Cleaning

Step 3: Transform

Step 4: Palantir Apps



Once source data is removed, deletions propagate

(ADMIN ONLY ACCESS)



LANDING ZONE

ANALYSIS ZONE



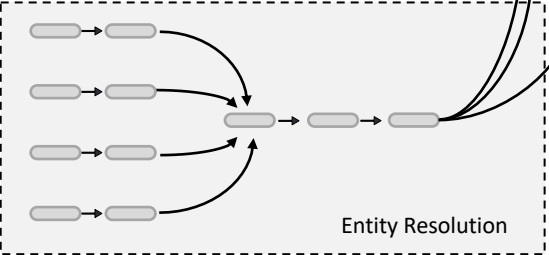
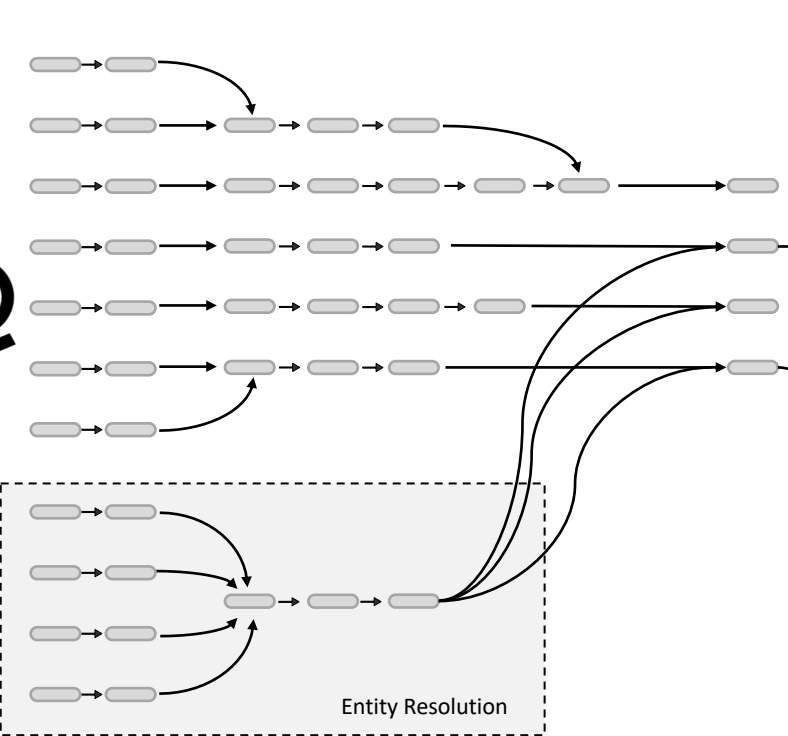
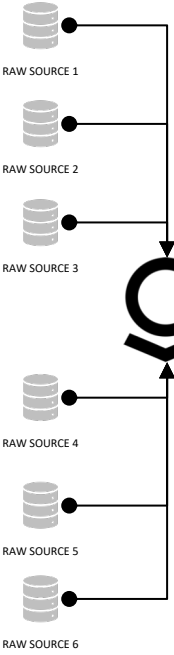
(USER ACCESS)

Step 1: Ingestion

Step 2: Cleaning

Step 3: Transform

Step 4: Palantir Apps



QUESTIONS

- Deletion techniques lie in a spectrum
- Reasonable “delete” standard across an ecosystem
- Balancing deletion with implementation cost
- Classifying non-active states of data

Thank You





WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Daniel DREWER
Data Protection Officer
EUROPOL
Eisenhowerlaan 73
NL-2517 KK The Hague

Brussels, **09 JUL 2018**
WW [REDACTED] /D(2018)1567 C 2018-0519

Dear Mr Drewer,

We would like to inform you that, as already announced orally, the EDPS has decided to open an own initiative inquiry. This inquiry concerns the data protection aspects of the contract signed between Europol and Capgemini Nederland B.V. concerning the use of Palantir technology to develop the Europol Analysis System in accordance with Article 43(2)(b) of the Europol Regulation (reference number 2018-0519). Please refer to this number in your correspondence with the EDPS.

For this inquiry, we would need a number of documents from your side. In this regard, we already have at our disposals the following documents (collected during our May inspection):

- The tender documents relating to the pre-qualification stage of the restricted procedure and as well as the tender specifications which were sent to these pre-qualified;
- The award decision, which encloses the evaluation report, concerning both the initial evaluation, which was cancelled, and the subsequent evaluation awarding, on 7 November 2012 the contract to Capgemini Nederland B.V (hereinafter Capgemini).

In addition, we would need the following:

1. The complete call for tenders concerning the two phases (the text of the call, the tender specifications, the draft contract and other annexes);
2. The offer made by Capgemini, including contractual relations with Palantir;
3. The contract signed between Capgemini and Europol including all annexes (tender specifications, offer, etc.) as well as any potential amendments.
4. The confidentiality agreement signed between Capgemini and Palantir;

5. Any other relevant documents concerning the obligation of Palantir when accessing personal data on Europol files.

Finally, it would also be very useful to receive a short summary of the main phases of the tender procedure for a better understanding (including the cancellation, the reasons etc.).

We would be grateful to receive this information by 14 September 2018 at the latest.

Yours sincerely,



Wojciech Rafał WIEWIÓROWSKI

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

In the Briefing note, Europol was however planning to revise the **ontology**⁴ of Palantir in a future release to include a property that would enable sensitive data to be easily retrievable.⁵ The target date for the revision was Q1 2018.

On 8 February 2018, during their bi-monthly meeting with Europol's Data Protection Function (DPF), my staff was however informed of several **setbacks** to the announced planning:

- The update of the ontology that will be performed in Q1 2018 will not address the previously described issue.
- No subsequent updates in relation to the creation of new properties to identify sensitive data are foreseen.

[REDACTED]

²

³

⁴

Ontology, in this context, is the model that describes the data stored for each entity relevant for an analysis

⁵

2) Compliance with the limitations on the processing of special categories of data subjects contained in the Opening Decisions of Analysis Projects

In the context of the inspection of December 2017, the EDPS was provided with a report from the DPF dated from September 2017⁶. This report refers to a compliance check performed by the DPF against the new EAS (Palantir) in order to identify data subjects entered without a personal implication. At the time, only Analysis Projects on counter-terrorisms had been migrated from [REDACTED] to Palantir. During the bi-monthly of 8 February, we were informed that the migration of all the other Analysis Projects was scheduled for later this month.

As stressed in that document, the **personal implication** specifies in which context a data subject is processed within Europol's databases. It allows ensuring compliance with Article 18 (5) and Annex II B of the Europol Regulation, which lists the categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in Article 18 (2), and with the Opening Decisions of the Analysis Projects which further specify which categories of data subjects can be processed in accordance with Article 18(3)(a) of the Europol Regulation.

[REDACTED]

The need for Europol to check manually whether all data subjects have been assigned a personal implication, together with the impossibility to obtain information on special categories of data subjects processed in each Analysis Project, affects the ability of Europol to ensure and of the EDPS to check whether the restrictions contained in the Opening Decisions with regard to the processing of special categories of data subjects are complied with.

* *
*

⁶ 'Data processing in the new EAS [REDACTED].

⁷ In the Briefing note mentioned above, Europol provided statistics on informants, victims, witnesses and minors stored for more than five years in [REDACTED] (for Analysis Projects on ex-AWF Serious and Organised Crime) on 1 October 2017 and stated that there was no such data stored in Palantir (for Analysis Projects on ex-AWF Counter-terrorism).

In view of the above, we have strong concerns about the ability of Europol to ensure compliance with the Europol Regulation in relation to the provisions on the processing of sensitive data and of specific categories of data subjects. These provisions are essential in the legal framework put in place by the Europol Regulation, which entered into force more than nine months ago. [REDACTED]

As you know, the EU legislator has entrusted the EDPS with the obligation to monitor and ensure the application of the Europol Regulation in relation to the processing of personal data by Europol (Article 43(2)(c)). These supervisory activities are subject to political scrutiny, which includes, at least once a year, the appearance of the EDPS before the Joint Parliamentary Scrutiny Group ("JPSG") to discuss general matters relating to the protection of personal data with regard to Europol's activities (Article 51 (2)(b)). The EDPS has been invited to appear before the JPSG for their next meeting, to be held on 19 March 2018.

In light of the fast approaching date of this meeting, and in order to be able to adequately answer any question that may be addressed to the EDPS in that regard, may I ask you to inform us about the actions that Europol intends to take to ensure that its processing operations are compliant with the Europol Regulation.

Sincerely yours,


Wojciech Rafał WIEWIÓROWSKI

Cc: Mr Daniel DREWER, Data Protection Officer, Europol



The Hague, 14 March 2018

EXECUTIVE DIRECTOR

European Data Protection Supervisor (EDPS)
Mr Wojciech WIEWIÓROWSKI
Assistant Supervisor

Via the Data Protection Function (DPF) at
Europol

Europol Analysis System (EAS) - Compliance with the Europol Regulation

Your letter, C 2018-0047, of 16 February 2018

Dear Mr Wiewiórowski,

Thank you for your letter of 16 February regarding data protection compliance matters affecting the EAS.



From an overall perspective, the delivery of the EAS, in view of the Europol Regulation which came into effect in May 2017 with new governance and compliance requirements, continuous human resource and budget constraints, as well as the technical complexity and required performance of the system to migrate the enormous amount of Europol's core analysis data to the new EAS, poses a continuous challenge to the organisation.

The EDPS is a key partner for Europol in upholding its high governance and data protection standards. I would like to express my appreciation and gratitude for the availability and cooperative approach of the EDPS, to work jointly with Europol in a proactive and constructive manner in order to address the data protection issues affecting Europol.

I have instructed my staff to take remedial action in relation to the areas highlighted in your letter, and, I attach, as an annex to this letter, an outline of activities which aims at providing you with assurance that Europol's processing operations will meet your compliance expectations, in line with the provisions of the Europol Regulation.

On the way forward, I propose that your feedback on the suggested remedial actions is discussed during the next bi-monthly meeting with the EDPS, in order to ensure that your expectations are satisfied. I have requested Europol's Data Protection Officer to inform me personally about the progress of the issues highlighted in your letter.

Yours sincerely,

Rob Wainwright
Executive Director

Outline: Europol Analysis System (EAS) – Compliance activities

1. [REDACTED]

[REDACTED]

[REDACTED], Europol will update the ontology of the Europol Analysis System (EAS), introducing a new property, specifically designed to capture sensitive data. This new property will include values to reflect all of the sensitive data categories referred to in Article 30 (2) of the ER (racial or ethnic origins, political opinions etc.).

The ontology update for the EAS will be implemented by the end of Q2 2018. At the same time, the pre-processing capability (referred to as [REDACTED]), for inserting data from SIENA into the EAS, will also be adjusted, in order to ensure that, at the time of Europol receiving data for analysis purposes, the respective sensitive data categories specified in Article 30 (2) ER are reflected in the data model, for subsequent processing in the EAS. Alongside the technical changes, Europol will provide awareness and training to all relevant staff, for making sure that the adjustments to the technology are understood and consistently applied in practice.

Concerning the assignment of sensitive data values to existing person data sets in the EAS, [REDACTED]

[REDACTED] contain sensitive data information attributes processed by Europol. This estimate is based on the number of free text comments fields filled in for person data sets, given that in the previous EAS, sensitive data attributes were kept in the free text 'comment field' (as outlined in the letter of the EDPS).

[REDACTED]

2. Compliance with Article 31 (3) of the Europol Regulation

In order to be able to inform the EDPS if sensitive data (Article 30 (2) of the ER) or special categories of data subjects, such as victims or witnesses (Article 30 (1) of the ER), are stored for more than five years, Europol envisages the roll-out of a new capability [REDACTED]

[REDACTED] Combined with the development of the Analytics Platform, it is envisaged to link the time period of more than five years under Article 31 (3) of the ER to the creation of the person data set in the EAS. [REDACTED]

[REDACTED]

3. Compliance with Article 18 (3) (a), 18 (5), Annex II B of the Europol Regulation

Concerning the EDPS' observation on the linking of a person data set to a specific Analysis Project, Europol would like to note that such a relationship can be identified indirectly, through the document object correlated with each person data set.

In order to improve the storing of data subjects with a mandatory personal implication attribute (as a suspect, witness, contact associates etc.), including a property to

denominate the relationship of a (person) data set to a specific Analysis Project (AP), Europol intends to create a compulsory quality check, before a user (analysis staff) can write the data in the database of the EAS.

The vendor has proposed a possible functionality to cover this feature. The maturity of technology solution announced from the vendor is being assessed, which will include a feasibility study that is launched in Q2/2018. As an interim measure, training and awareness sessions for analysis staff and weekly monitoring of EAS data insertion, especially concerning data subjects to ensure a consistent assignment of personal implications for person data sets, is undertaken.





The Hague, 21 September 2018

European Data Protection Supervisor (EDPS)

Mr Wojciech WIEWIÓROWSKI
Assistant Supervisor

Cc: Mr Daniel Drewer
Data Protection Officer (DPO) of Europol

Inquiry regarding compliance of the new Europol Analysis System with Europol Regulation (EDPS case 2018-0047) and

Inquiry regarding data protection aspects in relation to the contractual relationship between Europol and Capgemini concerning the use of Palantir technology to develop the Europol Analysis System (EDPS case 2018-0519)

Dear Mr Wiewiórowski,

Given my role as Security Coordinator of Europol, I have been asked by the Executive Director to respond to the above two inquiry cases of the EDPS. I would like to provide you with a reply as follows:

EDPS Case 2018-0047

Concerning the three (3) identified main areas of required improvements, namely:

- (a) the processing of sensitive data (inclusion of data property fields in the Europol Analysis System (EAS) 3.0 to reflect all of the sensitive data categories referred to in Article 30 (2) of the Europol Regulation, such as racial or ethnic origins, political opinions etc.), the
- (b) linking of the categories of data subjects (person implications) in the EAS 3.0 to sets of particular Analysis Projects (APs) as per the related opening decisions of the APs (Article 18 (3) (a), Article 18 (5) and Annex II B of the Europol Regulation) and
- (c) the statistical reporting requirements for data processing (Article 31 (3) of the Europol Regulation) beyond 5 years,

the implementation of the envisaged actions, as per Europol's update provided in March 2018, is delayed. The main reason is that Europol has decided in July 2018 not to roll out the EAS 3.0 to the Serious and Organised Crime (SOC) related APs,

I am enclosing for your convenience the related detailed report that was submitted to the Management Board (MB) Working Group (WG) on Information Management (IM). The report is provided for the background information of the EDPS only, thus not for further dissemination, in particular given that the matter will be addressed to the forthcoming Europol plenary MB meeting on 3 October 2018.

EDPS case 2018-0519

As regards your request regarding the data protection aspects of the contract signed between Europol and Capgemini concerning the use of Palantir technology to develop the EAS, please be provided with the following update:

EDOC #993651

Page 1 of 2

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

www.europol.europa.eu
Phone: +31(0)70 302 50 00
Fax: +31(0)70 302 58 96

**Europol Unclassified – Basic Protection Level
Releasable to the European Data Protection Supervisor (EDPS)**

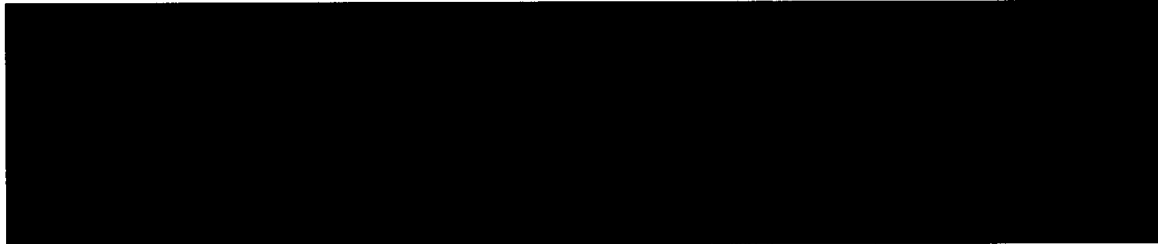
Europol has used customised Palantir Gotham software for analysing operational data as part of Task Force 'Fraternité' in 2016 (investigations following the terror attacks in Paris in November 2015), and since mid-2017, Europol has been using Palantir for the operational analysis of all counter terrorism related data.

Palantir software is a tool for operational analysis at Europol, in particular for the visualisation of data sets and to identify new lines of investigation in support of the competent authorities in EU Member States and beyond.

Europol has an indirect contractual relationship with Palantir, being a sub-contractor under a framework contract concluded with Caggemini.

The contractual relationship with Palantir as a sub-contractor is based on a public tender which followed the procurement rules applicable to Europol.¹

The tender was completed in 2012, and the related framework contract was signed in December 2012. The maximum value of financial expenditure under the framework contract is 7.5 Million Euro. The framework contract is due to expire in December 2019.



We are fully committed to ensure that all data storage and processing at Europol is in line with the applicable rules, including on data protection. A key principle is that Europol must observe the data ownership of the provider of the data, as a fundamental principle for trust and data sharing among law enforcement authorities.

Against this background, operational data, or copies of operational data sets, have not been, and will not be made available to Palantir as a private contractor for providing analysis software services. Private contractors also do not process or maintain Europol's operational data. Therefore, Palantir (or any other private company) does not hold Europol operational data.

In light of the volume of the information and its related sensitivity, I would kindly like to invite you, given the request expressed in your letter, to consult the aforementioned contract documentation at Europol's premises, should you still feel the need to do so, further to the information provided in this letter.

I trust that this information answers both your inquiries.

Please do not hesitate to get back to me should you have additional questions.

Yours sincerely,

Oldřich Martinů

Deputy Executive Director in charge of the Governance Directorate
Security Coordinator

Attachment: Europol Analysis System (EAS) – Analytical Capabilities Evolution (ACE) - Update from Europol (Report to the MB and IMWG)

¹ The related overall information is available on the so called "Tenders Electronic Daily Platform": <https://ted.europa.eu/udl?uri=TED:NOTICE:526287-2017:TEXT:EN:HTML&src=0>



WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Ms Catherine DE BOLLE
Executive Director
EUROPOL
Eisenhowerlaan 73
NL-2517 KK The Hague
Netherlands

02 AUG 2018

Brussels,
WW[redacted]sn/ D(2018)1813 C 2018-0047
Please use edps@edps.europa.eu for all
correspondence

Subject: Inquiry - Compliance of the new Europol Analysis System with Europol Regulation

Dear Ms De Bolle,

By letter of 16 February 2018 to Mr Wainwright, the EDPS launched an own initiative inquiry concerning the compliance of the new Europol Analysis System (EAS), i.e. Palantir Gotham, with the Europol Regulation (ER). In our letter, we raised two main areas of concern regarding respectively [redacted] and on the processing of special categories of data subjects contained in the Opening Decisions of the Analysis Projects (Articles 18(3)(a), 18(5), 31(3) and Annex II.B ER).

Mr Wainwright replied by letter of 14 March 2018, which enclosed an outline of the actions scheduled by Europol towards compliance.

My staff had also the opportunity to further tackle this matter during the bi-monthly meeting at Europol on 24 April 2018 (which involved a hands-on demonstration of Palantir Gotham as well as discussions on pending issues and possible ways forward) and during our annual inspection of 22-25 May 2018.

As you know, the next meeting of the Joint Parliamentary Scrutiny Group ("JPSG") of Europol will take place on 24-25 September 2018 in Brussels. In accordance with Article 51(2)(b) ER, the EDPS has been invited to appear before the JPSG on 25 September 2018. In order to be able to answer any question that the JPSG may address to us, could you please provide us with an update of the actions that Europol has taken on this matter to ensure full compliance of their operations with the Europol Regulation? Thank you.

Sincerely yours,

Wojciech Rafał WIEWIÓROWSKI

Cc: Mr Daniel DREWER, Data Protection Officer, Europol

From: [REDACTED]
Sent: 23 April 2018 14:25
To: [REDACTED]
Cc: EDPS-TECH-PRIVACY
Subject: RE: Meeting with Palantir

Dear colleagues,

Here is the case file number

 [REDACTED] [Meeting with Palantir on privacy](#)

Kind regards

[REDACTED]

From: [REDACTED]
Sent: 23 April 2018 14:10
To: [REDACTED]
Cc: EDPS-IT-POLICY
Subject: RE: Meeting with Palantir

Dear colleagues,

I have sent an email to the contact persons I received for a meeting with Palantir (vs privacy). It would be great if we had this meeting before the inspection but given the month of May, I doubt this would be possible (but you never know). I will of course keep you informed but if you could make sure your calendar is up-to-date and visible to me, that would ease the organisation of this meeting.

I have also requested a case file be open (and I put all of you as case officers to ensure you have access) and will communicate the number as soon as it is available.

Kind regards

[REDACTED]

From: [REDACTED]
[REDACTED]
Sent: 18 April 2018 16:44
To: [REDACTED]
[REDACTED] >
Cc: [REDACTED]
[REDACTED] >
Subject: Meeting with Palantir

[REDACTED]

Great to see you yesterday at the Biometrics Institute event. Having spent so many years steeped in GDPR, it was interesting to present to a room full of people who were much less familiar with it (although also perhaps slightly troubling that they were not a little more informed!).

I wanted to reach out to ask if EDPS would be

interested in meeting with some of our engineers and taking a closer look at some of the technical approaches that we are taking to privacy and civil liberties protective technologies. As I mentioned in my presentation, we have been developing these capabilities for a while, but we are continuing to adapt them for different customers as we help them meet GDPR requirements in a variety of contexts. I think feedback from some of the EDPS technical experts would be very welcome, and I know that our engineers would enjoy a more in depth discussion of some of these capabilities.

Would this be something of interest? I know this is a busy time for you (I can only imagine!), but we can be fairly flexible on dates as I and several of my colleagues are based in the UK and Europe. I look forward to meeting again soon!

■

■

■

Palantir Technologies

From: [REDACTED]
Sent: 23 April 2018 14:10
To: [REDACTED]
Cc: EDPS-TECH-PRIVACY
Subject: RE: Meeting with Palantir

Dear colleagues,

I have sent an email to the contact persons I received for a meeting with Palantir (vs privacy). It would be great if we had this meeting before the inspection but given the month of May, I doubt this would be possible (but you never know). I will of course keep you informed but if you could make sure your calendar is up-to-date and visible to me, that would ease the organisation of this meeting.

I have also requested a case file be open (and I put all of you as case officers to ensure you have access) and will communicate the number as soon as it is available.

Kind regards

[REDACTED]

From: [REDACTED]
[REDACTED]
Sent: 18 April 2018 16:44
To: [REDACTED] >
Cc: [REDACTED]
[REDACTED]
Subject: Meeting with Palantir

Christian –

Great to see you yesterday at the Biometrics Institute event. Having spent so many years steeped in GDPR, it was interesting to present to a room full of people who were much less familiar with it (although also perhaps slightly troubling that they were not a little more informed!).

I wanted to reach out to ask if EDPS would be interested in meeting with some of our engineers and taking a closer look at some of the technical approaches that we are taking to privacy and civil liberties protective technologies. As I mentioned in my presentation, we have been developing these capabilities for a while, but we are continuing to adapt them for different customers as we help them meet GDPR requirements in a variety of contexts. I think feedback from some of the EDPS technical experts would be very welcome, and I know that our engineers would enjoy a more in depth discussion of some of these capabilities.

Would this be something of interest? I know this is a busy time for you (I can only imagine!), but we can be fairly flexible on dates as I and several of my colleagues are based in the UK and Europe. I look forward to meeting again soon!

[REDACTED]

[REDACTED]

[REDACTED]

Palantir Technologies

From: [REDACTED]
Sent: 23 April 2018 08:40
To: [REDACTED]
Cc: [REDACTED]; EDPS-TECH-PRIVACY
Subject: RE: Meeting with Palantir

Hello,

This is definitely an opportunity we must seize. I think all Europol-related staff should participate. Count me in !

How do we set this up? Do we go through [REDACTED]? Or someone else? Or directly to the Palantir contact in the email?

Kind regards

[REDACTED]

From: [REDACTED]
Sent: 20 April 2018 18:10
To: [REDACTED]
Cc: [REDACTED]; EDPS-IT-POLICY
Subject: Re: Meeting with Palantir

Dear [REDACTED],

Thank you for the email. Palantir again and its the topic for the next Europol inspection! I believe that at least one of us (if not all!) should go if a meeting is scheduled. Of course I am interested

Kind regards

[REDACTED]

On 20 Apr 2018, at 17:51, [REDACTED] > wrote:

[REDACTED],

Would this be of any interest?

Kind regards

[REDACTED]

[REDACTED]

[REDACTED]

Von: [REDACTED] <[u](#)>
Datum: 20. April 2018 um 17:44:21 MESZ
An: [REDACTED] >
Kopie: [REDACTED] >
Betreff: Aw: Meeting with Palantir

Other than "scary creepy sh*t"? (not my copyright, sadly:
<https://boingboing.net/2018/02/27/new-orleans-police-used->

[predic.html](#) ;))

I guess it is not very likely that we'll be given anything other than spin (also judging from the email) but if a meeting is set up, perhaps colleagues involved with BTLE could benefit? I'm thinking [redacted] and [redacted] mainly on our side. But also the Europol team (didn't they try to use their technology at some point?)

Many thanks,

[redacted].

Excuse the brevity - sent from my mobile device

Dnia 20.04.2018 o godz. 17:24 [redacted]

<[redacted]> napisał(a):

would you like to meet and try to find out what these people actually do?

From: [redacted]

Sent: 18 April 2018 16:44

To: [redacted]

Cc: [redacted]

[redacted]

Subject: Meeting with Palantir

[redacted]

Great to see you yesterday at the Biometrics Institute event. Having spent so many years steeped in GDPR, it was interesting to present to a room full of people who were much less familiar with it (although also perhaps slightly troubling that they were not a little more informed!).

I wanted to reach out to ask if EDPS would be interested in meeting with some of our engineers and taking a closer look at some of the technical approaches that we are taking to privacy and civil liberties protective technologies. As I mentioned in my presentation, we have been developing these capabilities for a while, but we are continuing to adapt them for different customers as we help them meet GDPR requirements in a variety of contexts. I think feedback from some of the EDPS technical experts would be very welcome, and I know that our engineers would enjoy a more in depth discussion of some of these capabilities.

Would this be something of interest? I know this is a busy time for you (I can only imagine!), but we can be fairly flexible on dates as I and several of my colleagues are based in the UK and Europe. I look forward to meeting again soon!

[REDACTED]



[REDACTED]

[REDACTED]

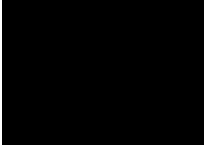
Palantir Technologies

From: [REDACTED] >
Sent: 01 June 2018 11:51
To: [REDACTED]
Cc: [REDACTED]; EDPS-TECH-PRIVACY
Subject: Re: Palantir meeting with EDPS on the 5th of June 2018 at 11 o'clock Ground floor meeting

Dear [REDACTED],

Many thanks for passing this along, that's very helpful.

The people in attendance on Tuesday will be:



I look forward to seeing you in Brussels soon.

Kind regards,

[REDACTED]

--

[REDACTED]

Palantir Technologies | Civil Liberties Engineer

[REDACTED] | [REDACTED]

From: [REDACTED] >
Date: Friday, June 1, 2018 at 3:25 AM
To: [REDACTED]
Cc: [REDACTED], EDPS-IT-POLICY <edps-it-policy@edps.europa.eu>
Subject: RE: Palantir meeting with EDPS on the 5th of June 2018 at 11 o'clock Ground floor meeting

Dear [REDACTED],

Thank you very much for your reply and confirmation. On our side, my colleagues just confirmed to have the meeting at 12 o'clock on Tuesday on the EDPS offices (Rue Montoyer 30 Brussels) . The meeting will take place on the ground floor meeting room. On your arrival , please ask for me at the security desk . On substance we would like (if possible) to be informed how Palantir takes into account :

- Privacy by design and default
- Data quality
- Data retention and deletion
- Security

Some other specific topics that have interest for us are :

- Palantir's functionality allowing **integration of open source data** (see at: <https://www.palantir.com/palantir-gotham/technologies/> "The Palantir Raptor service provides **in-place federated searching of external data sources.**")
- If/how Palantir is **flexible to accommodate different criminal justice requirements** that have to be translated into technical ones
- if/how your customers **can retain control on Palantir**

Please do not hesitate to contact me for any additional information.

Kind regards

[REDACTED]

From: [REDACTED]

Sent: 31 May 2018 16:03

To: [REDACTED]

Cc: [REDACTED]

Subject: Re: Palantir meeting with EDPS on the 5th of June 2018 at 11 o'clock Ground floor meeting

Dear [REDACTED],

My apologies for the belated response. A two-hour time frame strikes me as reasonable. Might 12-2pm be an option? If not, 11am-1pm works for us too, but 12-2pm might be easier in terms of travel.

Resource-wise we would only need access to WiFi and a projector. If at all possible it would also be helpful if [REDACTED] or one of his colleagues could circulate a list of topics in advance of the meeting that they would be particularly interested in covering. Otherwise we would probably provide a general introduction to Palantir, our approach to privacy protection as well as some concrete examples from our experience working with customers on implementing EU data protection law in practice.

Many thanks for organizing and for confirming the final timeframe as well as topics of interest. Please do not hesitate to reach out should you have any further questions.

Kind regards,

[REDACTED]

--

[REDACTED]

Palantir Technologies | Civil Liberties Engineer

[REDACTED]

From: [REDACTED]

Date: Thursday, May 31, 2018 at 8:55 AM

To: [REDACTED]

Cc: [REDACTED]

[REDACTED]

Subject: RE: Palantir meeting with EDPS on the 5th of June 2018 at 11 o'clock Ground floor meeting

Dear [REDACTED],

As I have not received any reply to my previous email, may I kindly ask you to confirm Palantir's presence to the EDPS offices next Tuesday morning so we can proceed to the organization of the meeting? I would also like to ask you to send us additional info about : 1) Duration of the presentation, 2) Any requirements from your side, 3) Exact time that is suitable for you .

For any additional information please do not hesitate to contact me.

Kind regards

[REDACTED]



[REDACTED] isor

Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels

[@EU_EDPS \[twitter.com\]](https://twitter.com/EU_EDPS)
[\[edps.europa.eu\]](http://edps.europa.eu)

www.edps.europa.eu

please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]
Sent: [REDACTED]
To: [REDACTED] >
Cc: [REDACTED] >
Subject: Palantir meeting with EDPS on the 5th of June 2018 at 11 o'clock Ground floor meeting

Dear [REDACTED]

On behalf of [REDACTED] who is currently absent, I would like to verify our planned meeting on the EDPS premises on the 5th of June.

My colleagues are looking forward to meet you. Could you please confirm your presence for the meeting and whether 11:00 is an appropriate time according your schedule.

Kind regards,

[REDACTED]





[REDACTED]



[REDACTED]



[REDACTED]

Eu isor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
 [@EU_EDPS \[twitter.com\]](https://twitter.com/EU_EDPS)  www.edps.europa.eu
[\[edps.europa.eu\]](http://edps.europa.eu)

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]

Sent:

25 January 2019 11:37

To: [REDACTED]

Cc: [REDACTED]

Subject:

Palantir Training

Signed By: [REDACTED]

[REDACTED]

Hope you are well. Our DPO passed on your request for Palantir administrator training, and we would be happy to set something up for you. There are a couple different Palantir platforms and the training can also differ with the particular context of a deployment, so it would be helpful to walk you through some of the options so we can get you the most relevant program. A number of us are going to be in Brussels next week for CPDP – are you planning to be at the conference? If not, we can also come by EDPS for a quick chat?

Look forward to catching up.

[REDACTED]

[REDACTED]

Palantir Technologies

“Live free or die: Death is not the worst of evils.” ~ General John Stark



[LGBTQ+ Ally](#)

[REDACTED]

From: [REDACTED]
Sent:
To: [REDACTED]
Cc:
Subject: Re: Palantir Admin Training
Signed By: [REDACTED]

Hi [REDACTED]

No need to bring any materials. We are just finalizing the schedule – I will get you the final hours by no later than EOB tomorrow.

Thanks!

[REDACTED]

[REDACTED]
Palantir Technologies

“Live free or die: Death is not the worst of evils.” ~ General John Stark



[LGBTQ+ Ally](#)

From: [REDACTED]
Date: Thursday, May 2, 2019 at 8:44 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Palantir Admin Training

Hi [REDACTED]

I hope this email finds you well. On my side, I prepared the administrative requirements to attend the training. Could you please let me know

- If I should bring any material related to Palantir or another technical field (standards, books on XXX)?
- The schedule for the training (hours)?

Thanks

[REDACTED] gards
[REDACTED]

From: [REDACTED]
Sent: 15 April 2019 15:43
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Palantir Admin Training

Training will be in our offices at 20 Soho Square. We'll be in touch with more details shortly!

[REDACTED]
[REDACTED]
Palantir Technologies

"Live free or die: Death is not the worst of evils." ~ General John Stark



[LGBTQ+ Ally](#)

From: [REDACTED]
Date: Monday, April 15, 2019 at 11:57 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Palantir Admin Training

Hi,

Great. I will book my tickets and hotel. Could you please tell me where the training will be held?
Thanks

[REDACTED]

From: [REDACTED]
Sent: 12 April 2019 21:03
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Palantir Admin Training

Let's go with Tues – Thu then. Go ahead and schedule for then and we'll be in touch shortly with the more detailed agenda. Thanks [REDACTED] – and sorry this has taken so long!

[REDACTED]
Palantir Technologies

"Live free or die: Death is not the worst of evils." ~ General John Stark



[LGBTQ+ Ally](#)

From: [REDACTED]
Date: Friday, April 12, 2019 at 3:03 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Palantir Admin Training

Hi,

The week of the 13th is OK for me. Any 3 days will do. Could you please let me know what would suit the trainer?

Thanks

[REDACTED]

From: [REDACTED]
Sent: 11 April 2019 22:00
To: [REDACTED]
Cc: [REDACTED]
Su

Yes! Again, apologies for the delay – people are hard to pin down. [REDACTED] and I actually herd cats just to unwind.

Are you available the week of May 13? We should be able to make any 3 days available that week. Let us know what works best for you!

[REDACTED]

[REDACTED]

Palantir Technologies

“Live free or die: Death is not the worst of evils.” ~ General John Stark



[LGBTQ+ Ally](#)

From: [REDACTED]
Date: Thursday, April 11, 2019 at 5:42 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Palantir Admin Training

Hi,

Any news from your side?

Regards

[REDACTED]

From: [REDACTED]
Sent: 03 April 2019 00:33
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Palantir Admin Training

Hi [REDACTED] At the moment, the news is that trainers are very difficult to pin down schedule-wise! But we are still working on getting someone for those early May dates. [REDACTED] or I will try to get this confirmed by the end of this week. Apologies for the delay.

[REDACTED]

Palantir Technologies

“Live free or die: Death is not the worst of evils.” ~ General John Stark



LGBTQ+ Ally

From: [REDACTED]
Date: Tuesday, April 2, 2019 at 12:51 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Palantir Admin Training

Hi [REDACTED]

Hope everything is OK. Do you have news for me?
Kind regards

[REDACTED]

From: [REDACTED]
Sent: 15 March 2019 00:35
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Palantir Admin Training

We will confirm dates with our trainers and get back to you next week. Thanks [REDACTED]

[REDACTED]

Palantir Technologies

"Live free or die: Death is not the worst of evils." ~ General John Stark



LGBTQ+ Ally

From: [REDACTED]
Date: Thursday, March 14, 2019 at 6:04 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Palantir Admin Training

Hello,

Thank you for the information. I have forwarded it and am waiting for a final answer from my colleagues which shouldn't be a problem.

I would love to set up the training in April if but the last half is already very busy. Can we do it early May (06-07-08)?

As for the request to [REDACTED] I have indeed made one, the reason being that at the time, I didn't know who could provide such a training (and I didn't know that you are in contact with all these partners). So I did things in parallel.

Unfortunately for [REDACTED] they provided a quote very late and it is way too expensive. I will reply to them today to cancel my request.

Could you please let me know if the dates I mentioned are suitable for you?

Thanks

[REDACTED]

From: [REDACTED]
Sent: 13 March 2019 11:48
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Palantir Admin Training

[REDACTED]

To answer your question, we do have an MSA with Europol. Although we are looking at this training as part of my team's general outreach efforts to parties interested in privacy, civil liberties, and data protection issues. So we are not really thinking of this as part of the Europol contract. We would (and have) offered this sort of training to academics, advocates, privacy officers, and others in the issue space as a means of helping to demonstrate what we do and get their feedback on our platforms.

On another note, we recently heard from one of our partners, [REDACTED], that they had also received a request from EDPS for training (this is standard – we work closely with our partners like [REDACTED] and they let us know as they receive such requests). We just wanted to double check if someone else from EDPS and/or another EU agency might also be looking for training? If so, we'd be happy to include them in your training.

In terms of dates for training – and mindful of your June deadline – what is your availability the last half of April? We could also find time in May if that is easier for you.

Thanks!

[REDACTED]

[REDACTED]

"Live free or die: Death is not the worst of evils." ~ General John Stark



[LGBTQ+ Ally](#)

From: [REDACTED]
Date: Wednesday, March 6, 2019 at 5:12 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Palantir Admin Training

Hi,

The outline is fine.

My finance team wanted to know if you have a framework contract with the EU Institutions. If so, could you please let me know which one?

Safe traveling

[REDACTED]

From: [REDACTED]
Sent: Tuesday 5 March 2019 09:58:46
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Palantir Admin Training

Great news [REDACTED] Is it just going to be you attending or did you have other colleagues who would be joining?

We'll figure out which of our trainers is available when and give you some options for dates. Does the outline that we provided below cover the main topics you wanted to learn? We'll provide a more detailed outline once we have the trainer(s) in place.

Please note – [REDACTED] and I are going to be in New York this week and then Australia next week, so please pardon any delays in getting back to you.

[REDACTED]

[REDACTED]

Palantir Technologies

"Live free or die: Death is not the worst of evils." ~ General John Stark



[LGBTQ+ Ally](#)

From: [REDACTED]
Date: Monday, March 4, 2019 at 4:54 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Palantir Admin Training

Hi,

Palantir Technologies

“Live free or die: Death is not the worst of evils.” ~ General John Stark



[LGBTQ+ Ally](#)

From: [REDACTED]
Sent: 01 June 2018 09:09
To: [REDACTED]
Cc: EDPS-TECH-PRIVACY; [REDACTED]
Subject: RE: Palantir Visit

Thank you, [REDACTED], noted.

As regards questions, [REDACTED] have already sent theirs to [REDACTED]. I will forward them to you in case you do not have them.

Kind regards,
[REDACTED]

From: [REDACTED]
Sent: 31 May 2018 16:20
To: [REDACTED]
Cc: EDPS-IT-POLICY ; [REDACTED]
Subject: RE: Palantir Visit

Dear all,

I just received confirmation that Palantir people will come for the presentation next Tuesday with a preference (due to travel limitations) for 12-2 as the exact timing .

If you don't have any objections I will send them a confirmation for 12. Repeating [REDACTED] 's request they ask us (if we want) to send them before some topics of interest for us , otherwise they will give a general introduction to Palantir, their approach to privacy protection as well as some concrete examples from their experience working with customers on implementing EU data protection law in practice.

Please, let me know your preferences.

Kind regards
[REDACTED]



[REDACTED]
[REDACTED]
[REDACTED]
Eu isor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
@EU EDPS www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]
Sent: 31 May 2018 15:58
To: [REDACTED]
[REDACTED]
[REDACTED]
Cc: EDPS-IT-POLICY <edps-it-policy@edps.europa.eu>; [REDACTED]
Subject: RE: Palantir Visit
Ok for me, very clear.
Thank you [REDACTED].
Regards,
[REDACTED]

From: [REDACTED]
Sent: 31 May 2018 15:56
To: [REDACTED]
[REDACTED]
[REDACTED]
Cc: EDPS-IT-POLICY <edps-it-policy@edps.europa.eu>; [REDACTED]
Subject: RE: Palantir Visit

Dear all,

I would like to update you on the Palantir visiting EDPS and presenting their tools and approach to privacy that was initially scheduled by [REDACTED] and is planned for next Tuesday morning. [REDACTED] has already booked the place (ground floor meeting room) for Tuesday morning at 11am and arranged a small catering. However, I already sent to the Palantir people two emails (one on Tuesday and another one today) to confirm their presence next week. Until now I have no confirmation. Nevertheless as we might have an answer before Tuesday I would propose to be ready and provisionally block your calendars (until further notice) for 11.

I would also like to invite you to think on potential questions related to privacy without mentioning Europol, although I suppose that the people that will come to us are aware of our activities.

Kind regards,

[REDACTED]



[REDACTED]
[REDACTED]
[REDACTED]
Eu isor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
[@EU_EDPS](https://twitter.com/EU_EDPS) www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]

Sent: 02 May 2018 11:19

To: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Subject: RE: Palantir Visit

Just FYI, we will have sandwiches and coffee!!!! :)

From: [REDACTED]

Sent: 02 May 2018 11:18

To: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Cc: [REDACTED]
[REDACTED]

Subject: RE: Palantir Visit

Dear colleagues,

Some topics that could be of interest:

- Data quality checking capacities of the core Palantir-Gotham product and of the main modules. Data quality checks in massive data intakes are of special relevance.
- Linked to the previous one, the way Palantir-Gotham deals with doubled (person) objects and their merging.
- Specific examples of how Palantir-Gotham follows the Privacy by Design and by Default principle.
- Data exporting capacities of the product.
- Does the core product or any available module have automated decision making capacities? Information on those capacities would be of interest.

Kind regards,

[REDACTED]

From: [REDACTED]

Sent: 02 May 2018 10:50

To: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Cc: [REDACTED]
[REDACTED] >

Subject: RE: Palantir Visit

Dear colleagues,

Palantir's guys confirmed that the 05/06 is suitable. They offered the opportunity to provide them with topics that we would like to discuss.

On their side they would like to present inter alia auditing analytics, deletion techniques, and accountable system principles

Let's seize the opportunity! :) Could you please send me the issues you think would be interesting to discuss? (the sooner the better)

Thanks

[REDACTED]

From: [REDACTED]

Sent: 27 April 2018 08:39

To: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] >

Cc: [REDACTED]
[REDACTED]

Subject: Palantir Visit

Dear colleagues,

Palantir got back to me with a couple of dates for their visit. One coincides with the away day and I know that no-one wants to miss that. So we are only left with the other date: 05/06/2018. Unfortunately, it is after the inspection but would still remain very interesting for us.

Could you please get back to me quickly on whether or not this date suits you?

Thanks in advance

Kind regards

[REDACTED]



EUROPEAN DATA PROTECTION SUPERVISOR

Case Reference
2017-0656

**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

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

HEAD OF ACTIVITY

SUPERVISOR

WIEWIÓROWSKI Wojciech Rafał	Assistant Supervisor
-----------------------------	----------------------

- 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..... 73

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. 2016/794¹ (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 data².

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 Europol³.

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).⁴ 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.⁵

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)⁶.
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 - O11 Operational Centre - Best Practices Manual for assigning officers²³;
- Europol, New AWF Concept, Guide for MS and Third Parties, 31 May 2012²⁴;
- AWF Case Manual²⁵.

4.1.3. Actions and findings

4.2. Data processing in Analysis Project Migrant Smuggling

4.2.1. Background

JSB inspection reports

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 victims⁶⁷, 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*).

67

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED¹⁷

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).⁶⁸

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 subjects⁶⁹ and sensitive data⁷⁰

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) ER⁷²;
- IDMC - Quick wins and urgent requirements⁷³ including notably rules on data review;
- The portfolio of APs⁷⁴, in particular the general section and the Opening Decision (OD) of the AP Migrant Smuggling;

- Analysis Work File Manual⁷⁵;
- DPF Audit - Data processing in the new EAS, September 2017⁷⁶
- Briefing Note “Road map for improving data quality and data protection compliance in Europol’s AWF”, 25 February 2016⁷⁷.

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

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED 20

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED²⁷

Recommendations	
No.	Content
<i>Recommendations concerning AP Migrant smuggling</i>	
	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.

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	
No.	Content
	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.

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 APs¹³¹, in particular the general section and the opening decision (OD) of AP Heroin;
 - input Manual¹³²;
-
- Road map for improving data quality & data protection compliance in Europol's AWF of 25 February 2016¹³⁵ 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 Policy¹⁷⁸;
- SIENA Use and Management policy¹⁷⁹;
- SIENA Data Retention Policy¹⁸⁰.

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 APs¹⁸⁶ (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**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 data¹⁸⁸ and of data subjects¹⁸⁹ stored for more than five years: this scenario does not trigger a legal obligation for Europol to conduct a review¹⁹⁰. If such personal data are stored for more than five years, Europol must **inform** the EDPS¹⁹¹. The AWF manual¹⁹² 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 deletion¹⁹³.

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 5¹⁹⁴;
- briefing note: Updated operational data review process (7/10/2016)¹⁹⁵
- IDMC – Quick wins and urgent requirements, section 3 – data review, 16 October 2017¹⁹⁶
- briefing note on special categories of personal data (6/11/2017)¹⁹⁷
- processing and handling procedures for basic support cases¹⁹⁸
- briefing note. Road map for improving data quality and data protection compliance in Europol AWF¹⁹⁹;
- manual for assessing contributions. Operational centre²⁰⁰.

4.5.3. Actions and findings

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

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 process²¹¹;
- Europol Operations Network Use Policy²¹²;
- Europol Security Manual²¹³;

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

5.1. Background

Europol developed the _____ to comply with Article 40 of the Europol Regulation (Logging and documentation). Through the _____, 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 AWFs²⁴⁰;
- Overall requirements²⁴¹;
- data protection statement²⁴²;

²⁴¹ EDOC-#932964-v1- _Overall_requirements_1_8.

²⁴² EDOC-#921889-v1- _Privacy_Statement.

- DPF Notification on ²⁴³.

5.3.Actions and findings

²⁴³ EDOC-#919158-v1A-DPF_Notification_

5.4. Conclusions and recommendations

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

No.	Content
	Inform all users 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.
	If the DPF were to use the audit the auditor function , 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.

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.*

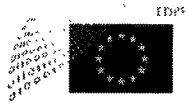
4. *The EDPS shall have the power to:*

- (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**

AFIS	Automated Fingerprint Identification System
AP	Analysis Project
AWF	Analysis Work File
CERT	Computer Emergency Response Team
CMR	Cross-match report
CORPNET	Corporate network
CT	Counter terrorism
DPF	Data Protection Function unit
DPO	Data Protection Officer
EAS	Europol Analysis System
ECD	Europol Council Decision 2009/371/JHA of 6 April 2009 establishing Europol
EDOC	Europol Document
EDPS	European Data Protection Supervisor
EIS	Europol Information System
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EMSC	European Migrant Smuggling Centre
ER	Regulation 2017/94 (Europol Regulation)
FP	Focal Point
GNST	General Nature and Strategic Type
IAM	Identity Access Management interface
IDMC	Integrated Data Management Concept
ISO	International Organization for Standardization
ITOC	IT Operational Centre
JSB	Europol Joint Supervisory Body
KPI	Key Performance Indicator
LEAs	Law Enforcement Authorities
MS	Member State
O1	Europol Front Office
OA	Operational Analysis
OAR	Operational Analysis Report
OCG	Organised Crime Group
OD	Opening Decision
OO	Opening Order
OWASP	Open Web Application Security Project
PeDRA	Personal Data in Risk Analysis
QUEST	Querying Europol Systems
SA	Strategic Analysis
SIEM	Security Information and Event Management
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SLA	Service Level Agreement
SOC	Serious and Organised Crime
SOCTA	Serious and Organised Crime Threat Assessment
SSSR	System Specific Security Requirements
TA	Thematic Analysis
THB	Trafficking of Human Beings
TP	Third Party
USE	Unified Search System



EUROPEAN DATA PROTECTION SUPERVISOR

Case Reference
2018-0067

**REPORT
ON
INSPECTION AT EUROPOL**

Conducted pursuant to Article 47(2) of Regulation (EC) No. 45/2001¹ 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
-----------------------------	----------------------

1. Summary 5

2. Scope 6

3. Methodology..... 6

4. Analysis and recommendations - Compliance with Regulation 2016/794..... 7

4.1. Europol Information System 7

4.1.1. Background 7

4.1.2. Criteria..... 8

4.1.3. Actions and findings..... 9

4.1.4. Conclusion and recommendations..... 15

4.2. Secondary Security Checks at Hotspots 16

4.2.1. Background 16

4.2.2. Criteria..... 19

4.2.3. Actions and findings..... 20

4.2.4. Conclusion and recommendations..... 24

4.3. Processing of persons under 18 in the Europol Analysis System..... 25

4.3.1. Background 25

4.3.2. Criteria..... 29

4.3.3. Actions and findings..... 37

4.3.4. Conclusions and recommendations 46

4.4. AP Travellers 55

4.4.1. Background 55

4.4.2. Criteria..... 58

4.4.3. Actions and findings..... 58

4.4.4. Conclusion and recommendations..... 64

4.5. Palantir Gotham (technical)..... 66

4.5.1. Background 66

4.5.2. Criteria..... 66

4.5.3. Actions and findings..... 67

4.5.4. Conclusion and recommendations..... 75

4.6. 77

4.6.1. Background 77

4.6.2. Criteria..... 77

4.6.3. Actions and findings..... 78

4.7. Information Security Management 81

4.7.1. Background 81

4.7.2. Criteria..... 82

4.7.3. Actions and findings..... 83

RESTREINT UE/EU RESTRICTED

4.7.4 Conclusion and recommendations..... 92

4.8. Testing and validation 94

 4.8.1. Background 94

 4.8.2. Criteria..... 94

 4.8.3. Actions and findings..... 95

 4.8.4 Conclusion and recommendations..... 96

5. Analysis and recommendations - Compliance with Regulation 45/2001 (Regulation 2018/1725) - Selection and recruitment..... 97

 5.1. Background..... 97

 5.2. Criteria 97

 5.3. Actions and findings..... 97

 5.3.1. Processing of data on disabilities and other data collected during the recruitment process 97

 5.3.2. Conservation of the certificate of good conduct 98

 5.3.3. Previous applications to a Europol post 98

 5.3.4. Retention period 98

 5.3.5 Right of access to their evaluation results by candidates 99

 5.4. Conclusions and recommendations 99

6. Compiled list of recommendations and deadlines for implementation..... 100

 6.1. List of recommendations 100

 6.2. Deadlines for implementation 106

Annex 1 – Powers of the EDPS..... 106

Annex 2 – Documents collected during the inspection..... 109

Annex 3 - List of abbreviations 120

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. 2016/794⁴ (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 data⁵.

To these ends, the EDPS fulfils the tasks and exercises powers provided for in Articles 57 and 58 of Regulation 2018.1725⁶ 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 the 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 Europol⁷.

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) ER⁸ (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 IDMC¹¹ 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 Guidelines¹² 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

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

4.2. Secondary Security Checks at Hotspots

4.2.1. Background

The **'hotspot approach'** was set up as part of the European Agenda for Migration⁴⁰, 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.

Under the corresponding current legal framework, Article 3 of the ER states that: ‘Europol shall support and strengthen action by the competent authorities⁴⁶ 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

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 office⁴⁷ 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 H2⁵⁰, 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.

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

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 concerned⁶⁶. These rules are included in a Portfolio containing the Opening Decisions (OD) of the APs⁶⁷ (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 ODs⁶⁸ 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

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

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 Manual⁷⁴;
- Europol Analysis System Manual (EAS Manual), Draft April 2018⁷⁵;
- 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.

⁷⁴ EDOC#660518v11.

⁷⁵ The AWF Manual is being updated to integrate the IDMC concept and other changes brought by the ER ("EAS Manual"). The last version sent by Europol is dated from April 2018. EDOC#886249-v3.

⁷⁶ EDOC#896347-v6 and EDOC#942003-v2.

⁷⁷ EDOC#819460 – v3.

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 2018⁷⁸;
- 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 1985⁸⁰;
- 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 justice⁸¹.

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.

⁷⁸ EDPS case numbers 2017-0451 and 2018-0223.

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

UN Resolution 44/25 of 20 November 1989. Article 1 defines "children" as "every human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier. The UNCRC is a legally-binding international agreement setting out the civil, political, economic, social and cultural rights of every child, regardless of their race, religion or abilities. In 2000, two additional protocols were added. One asks government to ensure children under the age of 18 are not forcibly recruited into their armed forces. The second calls on states to prohibit child prostitution, child pornography and the sale of children into slavery. A third armed protocol was added in 2001. This enables children whose rights have been violated to complain directly to the UN Committee on the Rights of the Child.

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

⁸¹ Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, 17 November 2010.

- 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

⁸² Declaration of the Rights of the Child (“Geneva Declaration of the Rights of the Child, adopted by the League of Nations in 1924 and adopted in an extended form by the United Nation in 1959).

⁸³ Article 1 UNCRC.

⁸⁴ EC Communication “An EU agenda for the rights of the child”, COM(2011) 60, Brussels, 15 February 2011

⁸⁵ UN Committee on the Rights of the Children, General comment No.14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para.1), p.3

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.

⁸⁶ EC Communication “An EU agenda for the rights of the child”, Brussels, 15 February 2011. See pp.6-7

⁸⁷ EC Communication “An EU agenda for the rights of the child”, Brussels, 15 February 2011

⁸⁸ Council of Europe, Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, “II. Definitions c”).

⁸⁹ CoE Guidelines on child-friendly justice, Explanatory Memorandum, para 31

- **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 children⁹⁰ and a Directive on special safeguards for suspects or accused persons in criminal proceedings who are vulnerable, including children⁹¹.

With regard to the **right to fair trial**, international instruments from the UN⁹² 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

⁹⁰ Directive 2012/29/EU of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime.

⁹¹ Directive (EU) 2016/800 of 11 May 2016 on procedural safeguards for children who are suspected or accused persons in criminal proceedings.

⁹² LIBE, EU Framework of Law for Children's Rights, 2012, p.9: Even if the EU is not party to the UNCRC, the EC has stated in the EU Agenda for the Rights of the Child that « standards and principles of the UNCRC must continue to guide EU policies and actions that have an impact on the rights of the child". In addition the CJEU has expressly recognized the need to respect children's rights and requires EU law to take due account of the UNCRC (see e.g. case C-540/03, European Parliament v. Council of the European Union [2006] ECR 5769, 37). All the MS have signed the Convention's two additional Operational Protocols on the sale of children, child prostitution and child pornography and on the involvement of children in armed conflict, but the EU has not.

⁹³ Principle 2.2(c).

⁹⁴ Commentary on Principle 1.

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

⁹⁵ Commentary on Principle 4

⁹⁶ Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, 17 November 2010.

⁹⁷ Foreword.

⁹⁸ Guideline III.E.1 and 2.

⁹⁹ Guideline IV.2.6.

¹⁰⁰ Para. 27.

¹⁰¹ Principle 8.1.

¹⁰² Commentary Principle 8.

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 108¹⁰⁵ 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

¹⁰³ FRA, Under watchful eyes: biometrics, EU IT systems and fundamental rights, p.68.

¹⁰⁴ Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, 17 November 2010.

¹⁰⁵ Council of Europe, Convention for the protection of individuals with regard to the processing of personal data (CETS No. 108), of 28 January 1981.

¹⁰⁶ Para. 57.

¹⁰⁷ Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

“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

¹⁰⁸ See e.g. T.Tridimans, *The general principles of EU Law*, 2nd ed., Oxford EC Law Library, p.139

¹⁰⁹ EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit*, 11 April 2017.

¹¹⁰ Principle 2.1 Council of Europe, Recommendation No R(87)15 regulating the use of personal data in the police sector. According to the Explanatory Memorandum (§43), “real danger” is to be understood as not being restricted to a specific offence or offender but includes any circumstances where there is a reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities.

¹¹¹ Council of Europe, Consultative committee of the Convention for the protection of individuals with regard to automatic processing of personal data, *Practical guidelines on the use of personal data in the police sector*, T-PD(2018)01, 15 February 2018.

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

DECLASSIFIED

DECLASSIFIED

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 activities¹⁶⁶, EDPS highlighted issues with Palantir, the new EAS for processing data of several APs, including AP Travellers¹⁶⁷. 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 EAS¹⁶⁸.

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 quality¹⁷⁵;
- 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 Manual¹⁷⁷;
- Draft EAS Manual¹⁷⁸.

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.
--	---

	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.
--	---

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

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 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 assessment²³⁰ or data protection impact assessment²³¹ 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 noncompliances 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.

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED 78

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 policy²⁷⁶ and the EDPS Guidelines on the rights of individuals with regard to the processing of personal data²⁷⁷.

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

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 her 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 and 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. ...".*

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

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
OI	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



EUROPEAN DATA PROTECTION SUPERVISOR

Case Reference
2019-0063

**REPORT
ON
INSPECTION AT EUROPOL**

pursuant to Article 57(1)(a) and (f), 58(1)(b), (d) and (e) of Regulation (EC) No 2018/1725
and Article 43(1) and (4) of Regulation (EU) No 2016/794

5 December 2019

EDPS
Supervision & Enforcement Unit
and
IT Policy Unit

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

INSPECTION TEAM

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

HEAD OF ACTIVITY**HEADS OF UNIT**

HAROU Delphine	Supervision & Enforcement
ZERDICK Thomas	IT Policy

ASSISTANT SUPERVISOR

WIEWIÓROWSKI Wojciech Rafał	Assistant Supervisor
-----------------------------	----------------------

- 1. Executive summary 6
- 2. Scope 7
- 3. Methodology 8
- 4. Analysis and recommendations - Compliance with Regulation 2016/794..... 9
 - 4.1. 9
 - 4.1.1. Background 9
 - 4.1.2. Criteria..... 11
 - 4.1.3. Actions and findings..... 12
 - 4.1.4. Conclusion..... 13
 - 4.2. 14
 - 4.2.1. Background 14
 - 4.2.2. Criteria..... 14
 - 4.2.3. Actions and findings..... 14
 - 4.2.4. Conclusion and recommendations..... 18
 - 4.3. 19
 - 4.3.1. Background 19
 - 4.3.2. Criteria..... 21
 - 4.3.3. Actions and findings..... 22
 - 4.3.4. Conclusion and recommendations..... 28
 - 4.4. 29
 - 4.4.1. Background 29
 - 4.4.2. Criteria..... 29
 - 4.4.3. Actions and findings..... 30
 - 4.4.4. Conclusion and recommendations..... 32
 - 4.5. 33
 - 4.5.1. Background 33
 - 4.5.2. Criteria..... 34
 - 4.5.3. Actions and findings..... 35
 - 4.5.4. Conclusion and recommendations..... 39
 - 4.6. 41
 - 4.6.1. Background 41
 - 4.6.2. Criteria..... 42
 - 4.6.3. Actions and findings..... 43
 - 4.6.4. Conclusion and recommendations..... 48
 - 4.7. 49
 - 4.7.1. Background 49

RESTREINT UE/EU RESTRICTED

- 4.7.2. Criteria..... 49
- 4.7.3. Actions and findings..... 49
- 4.7.4. Conclusion and recommendations..... 50
- 4.8. Follow-up to inspection report of 8 May 2018 (December 2017 inspection)..... 51
 - 4.8.1. Background 51
 - 4.8.2. Actions, findings and status of the recommendations..... 51
- 4.9. Follow-up to inspection report of 19 December 2018 (May 2018 inspection)..... 55
 - 4.9.1. Background 55
 - 4.9.2. Actions, findings and status of the recommendations..... 55
- 5. Analysis and recommendations - Compliance with Regulation 2018/1725..... 58**
- 6. Compiled list of recommendations and deadline for implementation..... 69**
 - 6.1. List of recommendations 69
 - 6.2. Deadline for implementation..... 74
 - Annex 1. Restricted information..... 75
 - Annex 2. Powers of the EDPS 80
 - Annex 3 – Documents collected during the inspection 83
 - Annex 4 - List of abbreviations..... 91

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of Regulation (EU) No 018/1725 (Regulation 2018/1725)¹ 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 2016/794² (Regulation 2016/794 or Europol Regulation or ER), the EDPS is specifically in charge of monitoring the processing of operational data by Europol and ensure compliance with Regulation 2016/794 and any other Union act relating to the protection of natural persons with regard to the processing of personal data by Europol.

Regulation 2016/794 applies to Europol's processing of operational data and Regulation 2018/1725 applies to Europol's processing of administrative data³.

To these ends, the EDPS fulfils the tasks and exercises the powers provided for in Articles 57 and 58 of Regulation 2018/1725 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 Regulations 2016/794 and 2018/1725.

The formal decision was communicated to Europol by means of an Announcement Letter dated 30 April 2019. The fieldwork was carried out between 3 and 6 June 2019 at the Europol premises in The Hague. The minutes of the inspection were sent to Europol for comments on 20 June 2019. Europol communicated their comments on 8 July 2019 (received by EDPS on 11 July 2019). The final minutes were sent to Europol on 29 July 2019.

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. Some restricted information is inserted in **Annex 1**.

¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies and agencies and on the free movement of such data, and repealing Regulation No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

² Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53.

³ Article 46 of Regulation 2016/794.

The recommendations contained in this report must be implemented to comply with Regulations 2016/794 and 2018/1725. The EDPS will carry out a close follow-up. If need be, powers listed in Annex 2 may be exercised.

This inspection was part of the EDPS annual inspection plan for 2019 and should be viewed as the final stage before formal enforcement action under Article 43(3) of Regulation 2016/794 and Article 58(2) of Regulation 2018/1725.

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

4.8. Follow-up to inspection report of 8 May 2018 (December 2017 inspection)

The EDPS carried out its first inspection at Europol between 12 and 15 December 2017 and issued an inspection report including 43 recommendations on 8 May 2018. The inspection team verified the implementation of selected recommendations of this report during the June 2019 inspection.¹⁶¹

4.8.2. Actions, findings and status of the recommendations

- **Recommendation** : *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.*

Findings and evaluation: The data model has been revised.¹⁶³

Status: closed¹⁶⁴.

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

RESTREINT UE/EU RESTRICTED

DECLASSIFIED

Annex 2. Powers of the EDPS

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

Article 58 Powers

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 her 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 and the 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 a 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 the 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 specified 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 on 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;*

- (b) to advise the controller in accordance with the prior consultation procedure referred to in Article 40, and in accordance with Article 41(2);*
 - (c) to issue, on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data;*
 - (d) to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 48(2);*
 - (e) to authorise contractual clauses referred to in point (a) of Article 48(3);*
 - (f) to authorise administrative arrangements referred to in point (b) of Article 48(3);*
 - (g) to authorise processing operations pursuant to implementing acts adopted under Article 40(4).*
- 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.*
- 5. The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedies and due process, set out in Union law.*

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

AD	Active Directory
AP	Analysis Project (or operational analysis project)
AWF	Analysis Work File
CFN	Computer Forensic Network
CORPNET	Corporate Network
DPF	Data Protection Function unit
DPO	Data Protection Officer
EAS	Europol Analysis System
ECB	Europol Cooperation Board
ECTC	European Counter-Terrorism Centre
EC3	Europol Cybercrime Centre
ED	Executive Director
EDOC	Europol Document
EDPS	European Data Protection Supervisor
EIS	Europol Information System
ENU	Europol National Unit
ER	Regulation 2017/94 (Europol Regulation)
IAM	Identity and Access Management
IDMC	Integrated Data Management Concept
JSB	Europol Joint Supervisory Body
LFE	Large File Exchange
MACR	Minimum Age of Criminal Responsibility
MS	Member State(s)
O1	Europol Front Office
OAR	Operational Analysis Report
OD	Opening Decision
OPSNET	Operational Network
PKI	Public Key Infrastructure
SIENA	Secure Information Exchange Network Application
SSSR	System Specific Security Requirement
TLS	Transport Layer Security
TP	Third Party

Report on the meeting with Palantir (June 5 2018)

On June 5 2018 a two hour interview was held with four staff members of Palantir. The profiles were mixed (two legal, one IT and one philosopher) and all of them were part of the same unit in the company. The unit is dedicated to include privacy and civil rights related capacities on Palantir products.

Main statements of the meeting

-) Palantir was founded in 2004 as a spin-off of PayPal. The company was created to take advantage of the tools that were developed to detect and prevent fraud in the context of PayPal business activities.
-) Their main products are Gotham and Foundry. Both tools analyse and provide intelligence from different databases but Gotham is designed to find relation among entities contained in them while Foundry is more oriented to discover correlations between different datasets.
-) Palantir is not an AI company, their business model is to develop and sell analysis products that help humans to make decisions. They have a small team (they didn't precise what small meant) working on Machine Learning (ML). The aim of this ML team is to develop tools that allow AI based information pre-processing when the amount of data is so huge that a human can't handle it.
-) Palantir is not the owner of the customer's data. The data is always kept under customers control in customers facilities or, at the customer's will, in an AWS service.
-) Palantir have customers not only on the law enforcement sector (e.g. Europol and Danish National Police), but also on other business niches like Health, Banking and Insurance.
-) Palantir's products are composed of a core package and optional modules. The core package is customized for each customer and they estimate that 80% of the setup comes out of the box while 20% must be customized.

Palantir specified that they sell the products on a flat rate and assume as losses any time spent above the estimated customization 20%.

-) Palantir is well aware that their tools can be dangerous and that's why they put a lot of effort in accountability. Palantir's approach to accountability is focused on the metadata¹ that is attached to the data included in the system.

Palantir claim that by using that metadata their customers can implement many of the principles of the GDPR like data storage limitation, accountability, data accuracy, purpose limitation and security. Palantir has developed some tools to help their customers to take advantage of those possibilities, but while some are included in the core package (security, authentication, audit logging and access control are part of it) some others are not and can be purchased by the customer.

-) Palantir allows their customers the customization of the product (e.g. defining new functionalities) by the use of Application Program Interfaces² (API).

¹ In this context, metadata means data related to the data included in Palantir (e.g. the date of insertion of the data or the last time some data has been accessed)

² In this context, an API is a software that must be used by Europol IT staff to access the data stored in Palantir's database.

) When asked if the system provides statistics (Europol was mentioned at this point) Palantir answered that they can be obtained. However, they put the responsibility on the customer's side, as they are the ones defining the ontology that allows for the definition of statistics.

) Palantir asked us for our experience on the proactive use of audit logs and any ideas on what kind of reports we think we would find useful.

It was stressed the relevance of proactive audit logging as pre-emptive medicine compared to reactive auditing were the patient is already ill. It was suggested that metadata could be used to develop a control for the automatic detection of unused data after certain amount of time.

) Palantir mentioned the concept of "Dynamic Data Minimization". Instead of presenting views of existing data to users depending on the user's rights, Palantir products works by dynamically creating new datasets with the data that a user is allow to access (e.g. The database could contain a property address and one user could be granted access to the city, while other to the complete address. Palantir creates datasets to show each user the appropriate piece of data).

) Palantir integrates data from different sources. Data (personal or not) goes through a series of transformations. Palantir systems keep the original data and the result of all the transformations, as these datasets have dependencies between them, managing the deletion of data becomes a difficult task.

They described their deletion process as 'tiered deletion'. The first step was a soft deletion (reclassification of data so the users can't access it) and the second one the hard deletion of the original data and of the result of all the transformations.

It was made clear that while the data controller keeps the data, it is processing data, no matter if the users can't access them.

After that they ensure that the process of fully deleting the data was not lengthy.

My personal impression is that they were trying to see if they could tell their customers that soft deleted data complies with the legal requirements related to deletion and cancelation of personal data.

) Palantir does not have any functionality related to anonymization. They basically told us that the process is to customer tailored to be easily included as part of the product.