24 May 2023

EUROPEAN DATA PROTECTION SUPERVISOR

Case Reference **2022-0749**

REPORT ON AUDIT PURSUANT TO ARTICLES 57(1)(a) and (f), 58(1)(b) of REGULATION (EU) 2018/1725

EUI concerned:

EUROPEAN BORDER AND COAST GUARD AGENCY (FRONTEX)

EDPS
Supervision & Enforcement Unit
and
Technology & Privacy Unit

AUDIT TEAM

[redacted]	Team leader, auditor (legal)
[redacted]	Head of Sector Area of Freedom, Security and Justice, auditor (legal)
[redacted]	Auditor (legal)
[redacted]	Auditor (legal)
[redacted]	Auditor (legal)
[redacted]	Auditor (IT)
[redacted]	Auditor (IT)

HEAD OF SECTOR AFSJ

[redacted]	Head of Sector Area of Freedom, Security and Justice

HEAD OF ACTIVITY AUDIT

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

HEADS OF UNITS

ZERDICK Thomas	Supervision & Enforcement
VELASCO Luis	Technology & Privacy

SUPERVISOR

WIEWIÓROWSKI Wojciech Rafał	European Data Protection Supervisor

CONTENTS

1. EXECUTIVE SUMMARY

Introduction

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of Regulation (EU) 2018/1725[1] (hereinafter referred to as the "Regulation 2018/1725") 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.

Article 86(1) of Regulation (EU) 2019/1896[2] (hereinafter referred to as the "EBCG Regulation") provides that the European Border And Coast Guard Agency ('Agency' or 'Frontex') shall apply Regulation 2018/1725 when processing personal data. Articles 86 to 91 of EBCG Regulation provide for specific data protection provisions further specifying the general provisions contained in Regulation 2018/1725 for the processing of personal data collected during Joint Operations, return operations, return interventions, pilot projects, rapid border interventions, migration management support team deployment (Article 88), in the framework of EUROSUR (Article 89), for the processing of operational personal data (Article 90) and in relation to data retention (Article 91).

To these ends, the EDPS fulfils the duties provided for in Article 57 of Regulation 2018/1725 and exercises the powers granted in Article 58 of the same Regulation. Among his powers to investigate, the EDPS can carry out investigations in the form of data protection audits. The power to audit is one of the tools established to monitor and ensure compliance with Regulation 2018/1725.

The EDPS' decision to conduct a data protection audit was communicated to Frontex by means of an announcement letter dated 6 September 2022. The fieldwork was carried out on 5 and 6 October 2022 at Frontex's

[1] Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies, OJ, L295, 21.11.2018, pp 39-98.

[2] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ, L 295, 14.11.2019, pp. 1-131.

premises in Warsaw. The minutes of the audit were sent to Frontex for comments on 27 October 2022. Frontex communicated its comments on 11 November 2022. The final minutes were sent to Frontex on 25 November 2022, and the Agency acknowledged their receipt on 7 December 2022.

Scope of the audit

Over the last few years, the role of Frontex has grown substantially. Frontex has become one of the largest EU agencies in terms of staff and budget and a key actor in EU border management moving from a merely coordinating and supporting role to a stronger operational one. Frontex now engages in activities involving increased processing of personal data, ranging from screening of migrants and return operations to combatting crime. The EDPS therefore sees the need to increase the monitoring of personal data processing activities by Frontex.

The focus of this audit was targeted on the activities conducted by Frontex in the context of Joint Operations and the processing of personal data collected in the context of the Processing of Personal Data for Risk Analysis (PeDRA) programme. The EDPS decided to focus on these activities as Joint Operations are the main source of personal data collected and further processed by Frontex. From a data protection perspective, these operations present risks linked to (i) the vulnerability of the individuals concerned by the processing, including those who have fled their own country because they were at risk of serious human rights violations and persecution there, (ii) the multiple purposes for which the data are collected and processed, which include the fight against cross-border crime, and (iii) the shared responsibility of the Member States and Frontex for EU border management.

The audit verified the compliance of Frontex's processing of personal data in the context of Joint Operations with Regulation 2018/1725 and the relevant provisions of the EBCG Regulation.

The audit focused in particular on the collection of personal data through debriefing interviews of persons intercepted while crossing external borders and their further processing by Frontex for the purposes of identifying suspects of cross-border crimes (including the exchange of these data with Europol), and for carrying out risk analysis.

In addition, the audit checked the implementation of the data protection by design and by default principle laid down in Articles 27 and 85 of Regulation 2018/1725, and checked compliance of the security of the systems for the processing of personal data resulting from the activities of screening and debriefing of persons intercepted while crossing the external borders.

Key findings of the audit

The audit identified 36 formal findings. The main findings are summarised below:

- **Debriefing interviews are the main source of personal data collection performed by Frontex**. Debriefing interviews are conducted in the framework of Joint Operations, which are carried out on the territory of Member States in cooperation with host Member State authorities. Interviews are performed on an ad hoc basis, with individuals intercepted while attempting to cross the EU's external border without authorisation. The purpose of debriefing interviews is to collect information about the interviewee's journey (modus operandi), reasons why they left their home country (so called 'push and pull' factors) and other information which may be relevant for Frontex risk analysis purposes. This information is compiled in debriefing reports which are stored in the Joint Operation Reporting Application (JORA) after their validation by the Intelligence Officer of the host Member State.

- During debriefing interviews, **Frontex also collects personal data about persons suspected of involvement in cross-border crime** (e.g. suspects of illegal immigration, human smuggling or other cross-border criminal activities) as reported by the interviewee (constituting operational personal data as defined by Article 3(2) of Regulation 2018/1725). This information, which forms part of the information extracted from the interview and compiled in debriefing reports, is shared with the analysts of Frontex' PeDRA (Processing of Personal Data for Risk Analysis) team for further dissemination to Europol. It is also redacted in view of its further processing for risk analysis by operational analysts in the Risk Analysis Unit.

- While Frontex considers information collected from interviewees and compiled in debriefing reports as anonymous, the EDPS finds that **information contained in some debriefing reports would allow for the identification of the interviewee and thus constitutes personal data** within the meaning of data protection law. The EDPS

welcomes the fact that Frontex Debriefing Officers do not include information about the name of the interviewee (or other direct identifier such as date of birth) in the debriefing reports as an important safeguard. However, the EDPS finds that merely excluding the name of the interviewee is insufficient to consider the information concerning him or her as anonymous data within the meaning of data protection law for the following reasons:

(1) In the case of some debriefing reports, the nature and extent of biographical and other detailed information about the interviewee reveals a combination of distinguishing features about that individual and their journey that would be sufficient to render those individuals identifiable.

(2) Interviewees may be indirectly identifiable from debriefing reports, including those which do not, on a standalone basis, contain identifying information on the interviewee, through the controller's access to additional information (pseudonymised personal data).

In light of the assessment that information collected in some debriefing reports on interviewees qualify as personal data as defined in Article 3(1) of Regulation 2018/1725, the EDPS issues recommendations to ensure that debriefing reports are subject to the standards and safeguards laid down in Regulation 2018/1725 and the EBCG Regulation.

- For the phase of the data processing, which consists in the collection of personal data via the debriefing interviews**, the EDPS finds that the host Member State and Frontex are joint controllers** as they both jointly define the purpose and the means of the processing (both of personal data of interviewees' as well as of operational personal data). According to Articles 28 and 86 of Regulation 2018/1725, joint controllers have to enter into a specific arrangement, laying down their roles and responsibilities, in particular towards the data subjects. The audit activities have shown that (i) the Operational and the Specific Activity Plans, which define the conditions for each type of operational activity developed, are incomplete as to the allocation of data protection responsibilities for the processing of operational data and (ii) there exists no arrangement between the joint controllers for the allocation of their respective data protection obligations regarding the processing of personal data of interviewees. Furthermore, the essence of the joint controllers' arrangements is not available to the data subjects. In order to ensure compliance with Articles 28 and 86 of Regulation 2018/1725, the EDPS has issued several recommendations and will closely monitor their implementation.

- The **EDPS has serious doubts concerning the compliance of debriefing interviews in their current form with the principle of fair processing** as provided by Articles 4(1)(a) and 71(1)(a) of Regulation 2018/1725. The EDPS finds that the conduct of debriefing interviews in their current form:
  (1) does not take sufficient account of the high vulnerability of the individuals targeted for data collection;
  (2) cannot guarantee the voluntary nature of the interview as they are conducted in a situation of deprivation (or limitation) of liberty, and are aimed at identifying suspects on the basis of the interviewee's testimony;
  (3) raises concerns as to whether the full implications of the interview and the subsequent handling of the data collected meets the reasonable expectations of the interviewees;
  (4) may result in the interviewee providing a self-incriminating testimony.

  Furthermore, the EDPS considers, in light of the highly sensitive nature of this activity, that Frontex should ensure that appropriate procedural safeguards are in place which take due account of the status of interviewees as detainees and are coherent with the law enforcement nature of the information and personal data collected. Such safeguards should protect the individuals concerned from adverse and disproportionate risks to their fundamental rights. In order to ensure compliance with Articles 4(1)(a) and 71(1)(a) of Regulation 2018/1725, the EDPS has issued several recommendations and will closely monitor their implementation.

- The **EDPS considers that Article 90 of the EBCG Regulation** read in the light of the provisions defining the Frontex's key role and its tasks **allows Frontex to process operational personal data collected only in the context of a specific and lawful purpose**, within its mandate, namely - in respect of debriefing interviews - for migration management purposes. Therefore, **the objective of the debriefing interviews cannot as such be directed at the gathering of operational personal data**. While Frontex is entitled to conduct debriefing interviews for migration management tasks, and might - in the course of such interviews - obtain personal data about suspects of cross-border crimes, **such collection should not alter the nature of debriefing interviews as migration management tools**.

  In addition, the EDPS considers that Frontex may not systematically, proactively and on its own collect any kind of information about

suspects of any cross-border crimes. This collection must be strictly **limited to identified needs of Europol, Eurojust and Member States competent authorities** and concern people (i.e. suspects of cross- border crimes) about whom Europol, Eurojust and Member State competent authorities are allowed to process personal data to perform their tasks.

In order to ensure compliance with Article 72 of Regulation 2018/1725, Articles 10 (1) (q) and 90 of the EBCG Regulation, the EDPS has issued several recommendations and will closely monitor their implementation.

The audit activities have also shown that **Frontex is automatically exchanging the debriefing reports with Europol without assessing the strict necessity of such exchange** as explicitly required by the EBCG Regulation (Article 90(2)a)). As this indicates a breach of Article 71 (1) (c) of Regulation 2018/1725 and Article 90 of the EBCG Regulation as well as of Article 15(3) and (4) of the Frontex Management Board Decision 58/2015, the EDPS has decided to open an investigation.

- **Frontex does not currently have the technical means to conduct searches of its systems containing debriefing reports, in order to retrieve personal data on a specific individual in response to a data subject access request**. This limitation imposes important obstacles to Frontex' ability to ensure data subject rights with regard to the information contained in debriefing reports, as it impedes the efficiency of handling data subject requests, and risks the accuracy of the outcome of searches performed for this purpose. As debriefing reports are the main source of personal data collected and processed by Frontex and concern very sensitive information (including information linking data subjects to serious criminal activity and which is processed without the data subject's knowledge of its collection), the effective exercise of data subject rights in this context is paramount. The EDPS has therefore issued a recommendation to ensure compliance with Article 17 and 80 of Regulation 2018/1725.

- The information contained in debriefing reports is used for purposes of risk analysis, in particular for the production of operational analysis reports and third countries analysis reports. The **EDPS has doubts as to whether the processing of personal data collected in the context of debriefing interviews is adequate, relevant and necessary in relation to the purpose of risk analysis**, in accordance with Article 4 (1) (c) of Regulation 2018/1725. This is due to

the low reliability of the data collected; lack of clarity regarding the methodology used to integrate debriefing reports into risk analysis products and overall usefulness of the information stemming from debriefing reports; and absence of a clear mapping and exhaustive overview of the processing of personal data and other sources of information which feed into the development of risk analysis products.

Furthermore, the EDPS has concerns regarding the use of information of low reliability for the production of risk analyses and its implications for certain groups who may be unduly targeted or represented in the output of risk analysis products. Such undue representation could have negative impacts on individuals and groups through operational actions as well as the policy decision-making process. In order to avoid a risk of non-compliance with Article 4(1)(c) of Regulation 2018/1725, and to avoid the risk of discrimination of certain group of people on the move due to the inaccuracy of the information collected during the debriefing interviews, in accordance with Article 80 of the EBCG Regulation, the EDPS has issued several recommendations and expects Frontex to implement them in light of the accountability principle.

- The implementation of Data Protection by Design and by Default ('DPbDD') encompasses several technical and organisational measures that must be implemented at the earliest stages of the design of the processing operations, and be in place throughout the processing, to provide for a robust implementation of DPbDD (Article 27 of Regulation 2018/1725). The **EDPS found that several elements which should be in place to provide for a robust implementation DPbDD are lacking in Frontex's software development processes**. These relate in particular to the conduct of Data Protection Impact Assessments (DPIA), the consultation of the Data Protection Officer (DPO) and the ability for the DPO to audit logs, as well as a procedure for testing with operational data.

  As per Article 33 of Regulation 2018/1725, controllers are required to **implement appropriate technical and organizational measures to ensure an appropriate level of security based on the risks associated with the processing of personal data**. To ensure compliance with this requirement, the audit team assessed the security measures implemented by the controller according to the ISO Standard 27002:2022. The assessment focused on five control objectives: Information Transfer, Access Rights, Management of Vulnerabilities, Secure Authentication, and Monitoring Activities.

The audit identified risks and shortcomings in this area. In particular, Frontex did not provide sufficient evidence (through a comprehensive risk assessment) that the security measures in place address the risks associated with the above control objectives to an acceptable level. The assessment highlighted some risks associated with the processing of personal data, such as the use of unencrypted email for the transfer of sensitive information, the use of only factor authentication, the fact that one of the systems was being operated without proper maintenance and awaiting decommissioning, and the insufficient monitoring of activities.

Recommendations and follow-up of the audit

As a result of the audit activities and his findings, the EDPS has issued a set of 32 recommendations addressed to Frontex. The main findings and recommendations are included at the end of each section of the report (with a full compiled list of recommendations inserted in Section 5). The recommendations contained in the report are issued in order to ensure compliance with Regulation 2018/1725 and relevant provisions of the EBCG Regulation.

In the case of 24 out of 32 recommendations, implementation is designated as imperative to ensure compliance with the legal framework and the EDPS has issued a deadline for implementation (ranging from immediate effect to the end of 2023) with the requirement that Frontex provides documentary evidence to the EDPS of implementation within the specified timeframe. The EDPS will carry out a close follow-up. If need be, enforcement powers may be exercised.

In addition, with regard to the exchange of operational personal data with Europol, the EDPS' findings indicate that Frontex has breached Article 71 (1) (c) of Regulation 2018/1725, Article 90 (2) (a) of the EBCG Regulation and Article 15(3) and (4) of the Frontex Management Board Decision 58/2015 by not assessing the strict necessity of sharing data packages with Europol, for the performance of its mandate. The EDPS has thus decided to open an investigation, which may result in the exercise of enforcement actions.

This audit was part of the EDPS Annual Audit Plan for 2022.

2. SCOPE

The audit aimed to monitor the compliance of Frontex's processing of personal data in the context of Joint Operations with Regulation 2018/1725 and relevant provisions of the EBCG Regulation.

The audit focused in particular on the collection of personal data through debriefing interviews of persons intercepted while crossing external borders and their further processing by Frontex for the purposes of:

(1) identifying suspects of cross-border crimes including the exchange of these data with Europol and,
(2) carrying out risk analysis.

Additionally, the audit aimed to check the implementation of the data protection by design and by default principle laid down in Articles 27 and 85 of Regulation 2018/1725, in particular for the processing of personal data resulting from the activities of screening and debriefing of persons intercepted while crossing the external borders.

Finally, the audit aimed to check compliance of the security of the systems underlying the processing of personal data resulting from the activities of screening and debriefing of persons intercepted while crossing the external borders with the requirements of Articles 33 and 91 of Regulation 2018/1725.

3. METHODOLOGY

On 29 and 30 March 2022, the EDPS conducted an operational visit at Frontex in order to get a better understanding of Frontex's activities and its role in the context of Joint Operations.[3] The visit consisted of presentations and exchanges with Frontex cross-departmental operational staff. The presentations and the follow-up discussions provided an insight into how Joint Operations are initiated, planned, organised and carried out as well as into the data processing they generate. They contributed to prepare for the audit.

The audit was performed in accordance with the procedures established in the **EDPS Audit Guidelines** and by relying on the cooperation of the staff members and managers of Frontex to provide requested information,

[3] Case file 2022-0414

data, documents and access to premises. This audit was part of the EDPS Annual Audit Plan for 2022.

In particular, **meetings and interviews** were set up and held with Frontex 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 Frontex staff constitute the basis for the observations and recommendations in this report.

Minutes of the meetings were drafted in order to document the audit procedures applied and provide for a transcript of the conversations with Frontex 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 Frontex for acknowledgment of receipt.
This **report** takes into account the documents provided by Frontex before the audit (listed in **Annex 2**) and during the on-site audit (listed in **Annex 3**), as well as documents requested during the on-site inspection and provided afterwards (the latter being listed in **Annex 4**).

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

4. ANALYSIS AND RECOMMENDATIONS

4.1. Processing of data in the context of Joint Operations

4.1.1 Background

One of the main tasks of Frontex is to assist Member States in circumstances requiring increased technical and operational assistance at the external borders by coordinating, organising and participating to Joint Operations.[4] Frontex may launch a Joint Operation upon a request from a Member State.[5] It can also recommend a Joint Operation to a Member State based on the results of its vulnerability assessment or risk analysis.[6]

All Joint Operations are set up in agreement with the host Member State (i.e. the Member State in which or from which a Joint Operation is

[4] Article 10 (1) (g) EBCG Regulation.
[5] Article 37 EBCG Regulation.
[6] Article 41 EBCG Regulation.

launched)[7] and based on an operational plan. The operational plan defines the aim of each Joint Operation. It covers all aspects considered necessary for carrying out the Joint Operation, including a description of the tasks and data protection requirements.[8]

[redacted]

As specified in Article 37 (4) of EBCG Regulation, the objectives of a Joint Operation may be achieved as part of a multipurpose operation including:

- coast guard functions (border surveillance: seaborne, airborne, terrestrial assets, supporting Search and rescue ('SAR') operations),
- the prevention of cross-border crime (focusing on the fight against migrant smuggling or trafficking in human beings) and,
- migration management (focusing on identification, registration, debriefing and return).

4.1.2. Criteria

The following provisions and recitals of the EBCG Regulation and Regulation 2018/1725 are of particular relevance for the EDPS analysis:

a) EBCG regulation

Joint Operations

[7] Article 2(20) EBCG Regulation.
[8] Article 38 (3) EBCG Regulation.

- Article 37 (4) on identification, registration and debriefing activities that Joint Operations may involve;
- Article 38 on the operational plan to be concluded between Frontex and the Member State in which the Joint Operation is launched; and
- Article 88 on the processing of personal data collected in Joint Operations.

Risk Analysis

- Article 29 providing the framework and modalities for conducting risk analysis (including Article 29(1) requiring that all personal data shall be anonymised in the results of annual and strategic risk analyses);
- Article 87(1)(e) providing for Frontex to process personal data for the purpose of risk analysis in accordance with Article 29;
- Article 88(1)(a) and (c) read in conjunction with Article 88(2)(e) providing for the processing of personal data of persons who cross the external borders without authorisation and specific categories of information linked to those persons, collected during Frontex operational activities where necessary for the preparation of risk analyses;
- Article 100(2)(e) with regard to the lists of mandatory information and data to be exchanged with Frontex by national authorities; and
- Recital 40 outlining the objectives and substance of Frontex risk analyses, to be based on a common integrated risk analysis model, to be applied by Frontex itself and by Member States.

Identification of suspects of cross-border crime in order to facilitate the exchange of information with the law enforcement authorities of the Member States, Europol or Eurojust

- Article 10 (1) (q) on Frontex's tasks to cooperate with Europol and Eurojust within their respective mandates and provide support to Member States in the fight against cross-border crime;
- Article 68 (1), (2) and (5) on the cooperation of Frontex with Union institutions/bodies/ offices/agencies, in particular the obligation to conclude working arrangements;
- Article 87 (1) (d) providing for Frontex to process personal data for the purpose of facilitating the exchange of information with law enforcement authorities of the Member States, Europol or Eurojust in accordance with Article 90;
- Article 90 on the processing of operational personal data by Frontex and their exchange with Europol, Eurojust and the competent law enforcement authorities of the member States ; and
- Recital 41 indicating that given its activities at the external borders, Frontex should contribute to preventing and detecting cross-border

crimes, where it is appropriate for it to act and where it has obtained relevant information through its activities, and coordinate with Europol which is the EU agency responsible in this area.

b) Regulation 2018/1725

- Article 3 (1) on the definition of personal data;
- Article 3 (2) on the definition of operational personal data;
- Article 3 (6) on pseudonymisation;
- Article 3 (8) on the definition of controllers;
- Articles 4 (1) (a) and 71 (1) (a) on the principles of lawfulness and fairness;
- Articles 4 (1) (c) and 71 (1) (c) on data minimisation;
- Article 27 on data protection by design and by default;
- Article 28 and 86 on joint controllers; and
- Articles 14 to 20 and 78 to 82 on the data subjects rights.

The EDPS also took into consideration in particular the following **Frontex internal and public documents for its analysis**:

- The Common Integrated Risk Analysis Model (CIRAM)[9]
- The Common Integrated Risk Analysis Model (CIRAM), limited, September 2021[10]
- Guidelines for Risk Analysis Units: Structure and Tools for the application of CIRAM version 2.0, 2012[11]
- Frontex public website webpage on situational awareness and monitoring[12] and operational analyses[13]
- Examples of Operational Risk Analyses provided by Frontex[14]
- Annual Risk Analysis 2021[15]
- Strategic risk analysis 2022[16]
- Strategic risk analysis 2020 (including the observation that "Information from Frontex debriefing activities indicates how the

[9] https://frontex.europa.eu/assets/CIRAM/en_CIRAM_brochure_2013.pdf
[10] 21.5050_CIRAM_F9_web_alternative numbering
[11] CIRAM Guidelines 2012 Interactive V6 (1)
[12] https://frontex.europa.eu/we-know/situational-awareness-and-monitoring/monitoring-risk-analysis/
[13] https://frontex.europa.eu/we-know/situational-awareness-and-monitoring/operational-analysis/
[14] 2022_Weeks 33-34_BIWAR JO Themis 2022; 2022_Week 36_WAO JO Themis 2022; 2022_Week; 35_WAO JO Themis2022;2022_JO_Focal_Points_biweekly_report_15.pdf; 2022_JO_Focal_Points_biweekly_report_14.pdf; 2022_JO_Focal_Points_biweekly_report_13.pdf.
[15] https://frontex.europa.eu/documents-and-publications/risk-analysis-for-2021-MmzGl0
[16] Frontex website - public register of documents

criminal economy intersects with militant and terrorist groups' economic and political ambitions")[17]
- Product Card: Annual Risk Analysis (ARA)[18]
- Frontex Rules of procedures[19]
- Frontex Management Board Decision 58/2015, Articles 3 (1) (b), 9 (2) and 15
- Frontex Management Board Decision 69/2021, Articles 6 (1) (b) and 9
- Frontex Management Board Decision 68/2021, Recital 6, Article 9 (2)
- JORA Incident Template Guidelines for Air Operations
- JORA Incident Template Guidelines for Sea Operations
- JORA Incident Template Guidelines for Land Operations
- Specific Activity Plan Joint Operation (JO) THEMIS 2022[20]
- Specific Activity Plan JO Focal Point Air, Amendment no. 1[21]
- Evaluation report JO THEMIS (pp. 8-10, 24-25, 27-28)[22]
- Sample of debriefing interview reports[23]
- Sample of JORA incident reports[24]
- RAU Division PowerPoint presentation - Briefing on targets: present and emerging trends at air borders
- Extracts from FRO monitoring report from Mission in Lesvos Greece from 28 February to 10 March 2022
- Handbook to the Operational plan, version June 2022
- Operational Plan, General plan Multipurpose operational activities in the Member State (MOA-MS), version 14.12.2021
- Specific Activity Plan, Amendment no 3, Joint Operation TERRA 2022, 12.07.2022 (Reg. No 13941C/2022)
- Specific Activity Plan, JO Poseidon 2022, 24.01.2022 (Reg. No 13947/2021)
- Working arrangement between Europol and Frontex, signed on 4 December 2015, Article 18
- Sample of debriefing interview reports[25]

---

17 Frontex website - public register of documents

18 Product_Card_ARA_V1.0 UPDATED

19 Frontex Internal Structure and Rules of Procedure ('FISRoP')

20 Specific Activity Plan Joint Operation (JO) THEMIS 2022

21 SAP - JO FP Air - 2022 - Amendment 1 (1)

22 FER JO Themis 2020 - Sensitive

23 Copies of 13 debriefing reports provided to the EDPS audit team during the audit

24 Live demonstration of four JORA incident reports shown to the EDPS audit team during the audit

25 11 debriefing interview reports (four debriefing interviews reports checked on the screen by the EDPS audit team during the audit activities and copies of seven additional debriefing interview reports provided to the EDPS audit team during the audit).

- Statistics on PeDRA transmissions from Joint Operations Terra and Themis to Europol and related number of Europol hits for the period of August 2021 to July 2022
- Statistics on PeDRA transmissions from all Joint Operations to Europol for the period of January 2022 to July 2022

4.1.3. Actions

In addition to the information gathered on the processing of personal data in the context of joint operations in general, including the involvement of different Frontex' divisions/units in the data flows regarding screening/debriefing and intelligence reports activities, the audit team conducted interviews and requested demonstrations on activities of Frontex in the context of the following Joint Operations: Terra, Focal Air points, Themis and Poseidon. The aim was to understand the objectives of the debriefing interviews, the risks and benefits associated with them and the practical organization of the interviews from the moment of planning up until the further use of data gathered during the debriefing interviews, either for risk analysis or law enforcement purposes in the context of these Joint Operations.

The EDPS interviewed Frontex team members responsible for conducting debriefing interviews, Frontex's staff members responsible for the use of information collected at the debriefing interviews, either for further transmission of operational data to Europol (PeDRA) or for risk analysis (in various forms). The EDPS had also a chance to interview three Fundamental Right Officer Monitors.

The Data Protection Office attended the interviews, which were followed by hands-on demonstrations.

All audit activities are described in detail in the audit minutes. The next section will focus on the most relevant audit activities and in particular on activities which triggered findings and recommendations.

4.1.4. Findings and recommendations

The following sections (4.1.4.1 to 4.1.4.6) present the EDPS findings and recommendations as regards the data collected during Joint Operations (section 4.1.4.1), the role of Frontex in this context (section 4.1.4.2), the way in which personal data are collected (section 4.1.4.3), the processing of these data for the purposes of identifying suspects of cross-border crime in order to facilitate the exchange of information with the law

enforcement authorities of the Member States, Europol or Eurojust (section 4.1.4.4) and for the purposes of risk analysis (section 4.1.4.6) as well as the exercise of their rights by the individuals whose data are processed by Frontex (section 4.1.4.5).

4.1.4.1. Data collected in Joint Operations

The interviews have shown that information collected during Joint Operations and further processed in JORA is mainly obtained through three types of reports, namely: Incident reports[26], Screening reports[27] and Debriefing reports[28]. The audit team also asked about Intelligence reports[29] referred to in the Operational plan and the Specific activity plans concluded between Frontex and the host Member States. This section details the nature of the information collected through each of these reports and assess to what extent these should be qualified as personal data collection.

A) INCIDENT REPORTING

[redacted]

[26] See Handbook to OPLAN - Version June 2022, - Frontex Operational Activities, Warsaw 01/06/2022, p.56 and following Version June 2022

[27] See The Concept of SCR DBR, PowerPoint presentation given by Frontex during the audit activities, Annex 4, document N°1.

[28] See Handbook to OPLAN - Version June 2022, Frontex Operational Activities, Warsaw 01/06/2022 p.113

[29] See Handbook to OPLAN - Version June 2022, Frontex Operational Activities, Warsaw 01/06/2022 p.113

[30] JORA Incident Template Guidelines - Sea Operations; JORA Incident Template Guidelines - Land Operations; JORA Incident Template Guidelines - Air Operations.

[31] Minutes, p.18 and 19. The JORA incident template Guidelines state that “The incident can be rejected at the last level of verification in case of inconsistency in the reported incidents.”

[32] Minutes, p.19

[redacted]

33 Minutes, p.18
34 Minutes, p.30
35 Minutes, p.19
36 Minutes, p.22
37 Minutes, p.22
38 Minutes, p.31
39 Minutes, p.31
40 Minutes, p.12

The EDPS audit team verified a sample of JORA incident reports (three non-validated and one rejected) and confirmed that those reports did not contain personal data.[41]

Frontex officers also showed the audit team on-screen examples of FTF reports. The EDPS audit team could observe that those reports did not contain personal data.[42]

The EDPS audit team did not check the content of [redacted] as these are only used for purposes of human rights monitoring and are not used by Frontex for risk analysis or for the purpose of identifying suspects of cross-border crime in order to facilitate the exchange of information with the law enforcement authorities of the Member States, Europol or Eurojust.

While the audit team found no evidence to indicate that personal data is being collected as part of JORA incident reporting, it nevertheless noted the possibility that personal data could be reported inadverten[redacted] Findings also indicated an absence of procedures in place to prevent such an occurrence. Explicit guidelines on excluding personal data from incident reports do not appear to be included RAU-issued guidance on completing the reporting templates[43] and the validation procedure as presented to the audit team appeared to focus primarily on checking for inconsistencies or flagging potential misconduct or fundamental rights violations.

Although Frontex possesses a legal basis under Article 88 of EBCG Regulation to process personal data on individuals intercepted while crossing border without authorisation, as well as other categories of data, for risk analysis purposes, any such processing must be limited to what is necessary for this purpose in accordance with Article 88(2)(c) and with the principle of data minimisation (Article 4(1)(c) of Regulation 2018/1725) and justified accordingly.

Finding 1	Based on the outcome of the verifications performed by the EDPS audit team, there is no evidence to indicate that personal data is being collected as part of JORA incident reporting.
Finding 2	Systematic checks on the inclusion of personal

[41] The reports consisted of one refusal of entry under JO Terra, two refusals of entry under JO Air, and one incident involving document fraud/exit at the Greek-Italy border.

[42] Minutes, p.31

[43] JORA Incident Template Guidelines - Sea Operations; JORA Incident Template Guidelines - Land Operations; JORA Incident Template Guidelines - Air Operations.

	data do not appear to be part of the validation procedure for incident reports and clear guidelines on excluding personal data from incident reports ([redacted] are missing from RAU-issued guidance provided to the EDPS audit team.

Recommendation

In order to avoid risks of non-compliance with Article 4(1)(c) of Regulation 2018/1725 and Article 88 of the EBCG Regulation, the EDPS recommends that Frontex:

Recommendation 1	Formalise checks on the absence of personal data during Frontex Situation Centre verification of JORA incident reports and include this procedural step in the guidance issued by the Risk Analysis Unit.

In light of the accountability principle laid down in Article 4(2) of Regulation 2018/1725, the EDPS expect Frontex to implement the above recommendation accordingly.

B) SCREENING REPORTS

[redacted]

The purpose of the **screening interviews** is to establish the presumed nationality of the interviewee in order to enable the host national authority [redacted]

44 Minutes, p.6
45 Minutes, p.15
46 Minutes, p.12

[redacted]

At the end of the process, national authorities insert in JORA reports with aggregated data, including statistics on [redacted]

According to Frontex, these reports do not include personal data.[48] They rather consist of an intelligence gathering exercise on migratory routes, origins [redacted]

[redacted]

Screening interviews only result in the sharing of aggregated information which is inserted into JORA and used as a source of information for risk analysis purposes.

c) Debriefing reports

Collection process

Contrary to screening interviews, **debriefing interviews** are performed on an ad hoc basis, with no time restriction, in the places where persons are held after being apprehended outside regular cross-border check points. They are then located either in detention centres or open camps, depending on the country of reception.

[redacted]

47 SAP JO Themis, p.18:
48 SAP JO Themis, p.18:
49 Minutes, p.7
50 Minutes, p. 7

[redacted]

[redacted]

[redacted]

[redacted]

51 Minutes, p.7

52 Minutes, p.13

53 Minutes, p.9, 15 and 20 where the analysts interviewed by the audit team explained that tactical analyses constitute a contribution produced by RAU towards the operational plan through ‘tactical Focused Assessments’.

54 Minutes, p.10

55 Minutes, p.10

56 Handbook to the Operational Plan, p.13.

57 Minutes, p.10 and 13 where the DO interviewed by the audit team specified that while the SAP Terra indicated that the collection of information and personal data related to activities of people smuggling networks as purpose for the debriefing activities, the DO mentioned that while interested in such information, this is a complementary goal, not the main one.

58 Minutes, p.10 and 13

59 Standard Operating Procedure: Reporting and pre-processing of information and operational personal data in the JORA interview report, p. 18; Handbook to the operational plan, Frontex operational activities, Version June 2022, Warsaw 01/06/2022, p.115; Refer also to EDPS minutes of the audit.

[redacted]

[redacted]

[redacted]

DbRs that are categorised as containing no personal data are transmitted directly to [redacted] for risk analysis purposes. Reports containing operational personal data are channelled [redacted] for processing and redaction. Frontex stated that only once personal data has been removed from those reports, are they made available for risk analysis.[65]

EDPS' assessment of the nature of the data collected in debriefing reports

Frontex's procedures for handling personal data from debriefing interviews are governed by the Frontex Management Board Decision 58/2015.[66] The Decision provides for the processing of personal data only of data subjects

60 Minutes, p.14

61 Minutes, p.13

62 Minutes, p.14.

63 Minutes, p.11 and 13, 14, 15.

64 Minutes, p.8.

65 Minutes, p.8 and p.19

66 Management Board Decision 58/2015 adopting Implementing Measures for processing personal data collected during joint operations, pilot projects and rapid interventions, 18 December 2015.

categorised as persons suspected by the Member State competent authorities of involvement in cross-border crime.[67]

The audit team assessed whether Frontex' internal rules and procedures concerning the collection of personal data in debriefing reports are complied with in practice, by checking:
(a) The treatment of personal data of persons suspected of involvement in cross-border crime [redacted];
(b)Whether the remaining data collected pertaining to the interviewee was anonymous, in accordance with Frontex internal procedures, or could constitute personal data.

In order to check compliance with the rules in force, the audit team performed verifications on a sample of 13 debriefing reports selected at random from JORA[68] (four marked as containing no personal data and nine marked as containing personal data of persons suspected of involvement in cross border crime).[69]

All 13 reports contained information about the interviewee e.g. nationality, sex, and in certain cases also ethnicity and religious affiliation, and described the different legs and modus operandi of his/her journey. In some cases, the reports included detailed descriptions of specific incidents that had arisen during the course of the journey. In none of the reports were the names (or other specific identification information such as travel document number, or date of birth) of the interviewees recorded.

Concerning (a) the treatment of personal data of persons suspected of involvement in cross-border crime, verifications confirmed that in the nine reports marked as containing personal data of persons suspected of involvement in cross border crime, and in line with Frontex internal procedures, the personal data in question (names, phone numbers, addresses, URLs) [redacted] in order to allow for redaction of the data prior to their transmission to operational analysts for risk analysis purposes.

---

[67] Articles 2(2)(f) and 4(3) of the Frontex Management Board Decision 58/2015.

[68] The debriefing interviews selected have been conducted in the context of JO Themis, JO Poseidon, JO Indalo.

[69] Interview report no. 9708, dated 31 July 2022; Interview report no. 9962 dated 19 August 2022; Interview report no. 9975 dated 19 August 2022; Interview report no. 10022 dated 22 August 2022; Interview report no. 10153 dated 30 August 2022; Interview report no. 10217 dated 1 September 2022; Interview report no. 10701 dated 27 September 2022; Interview report no. 10787, dated 2 October 2022; Interview report no. 10769, dated 30 September 2022; Interview report no. 10781, dated 2 October 2022; Interview report no. 10614, dated 23 September 2022; Interview report no. 10640, dated 24 September 2022; Interview report no. 10771, dated 30 September 2022.

Data contained in debriefing reports that indirectly identify the interviewee

As regards (b) the nature of the information included in debriefing reports pertaining to the interviewee, Frontex considers that the lack of information directly identifying the interviewee (e.g. a name) in the debriefing report is sufficient to qualify these reports as containing no personal data on the interviewee .[70] This means that, according to Frontex, this information is considered as falling outside the scope of data protection law and is currently handled accordingly.

Article 3(1) of Regulation 2018/1725 defines personal data as any information relating to an identified or identifiable person who can be identified, directly or indirectly in relation to that information. According to Article 3(1), information enabling the identification of a data subject can include identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Recital 16 of Regulation 2018/1725 further provides that personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly.

It follows from the above that while identification through a name is the most common means, it is not necessary in all cases to identify an individual.[71] While an individual may be directly identified through a name, they may be indirectly identifiable through other pieces of information which hold a particularly privileged and close relationship with an individual, including those examples referenced in Article 3(1) of Regulation 2018/1725 ("*one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person...*". A person may be identified indirectly through one of these identifiers, or a combination of significant criteria which allows him or her

[70] See Handbook to OPLAN - Version June 2022, Chapter 15.

[71] Article 29 Data protection Working Party, Opinion 4/2007 on the concept of personal data, pp.13 and 14.

to be recognised by narrowing down the group to which he or she belongs (age, occupation, place of residence, etc.).[72]

It is thus not sufficient for debriefing reports to exclude pieces of information that directly identify the interviewee in order for the report to be considered as anonymous. It should also be established that these reports do not contain information indirectly identifying the interviewee.

During the checks performed by the audit team, the EDPS found that several of the debriefing reports contained not only detailed information on an individuals' journey (routes, modus operandi, and details of specific incidents en route) but also detailed biographical information on the interviewee, as well as on their family members. Such information included their place of prior residence (name of town or village), age, marital and familial status, children's ages and genders, occupation and information related to their professional career, years during which military service were performed as well as very specific biographical details (such as incidents relating to family disputes, health status of family members etc.).

Of the 13 reports checked, the EDPS identified four reports which contained a high level of biographical detail on the interviewee.[73] These included the testimony of one [redacted] interviewee which included extensive detail of his life in the years leading up to his departure to the EU, including various places of residence documented by year and duration; occupations; family information.[74] [redacted]

Another such report included very specific information not only about the interviewee himself, [redacted] but also about his family members [redacted]

[72] Ibid, pp. 12-13.

[73] Debriefing report No 10771; debriefing report No 10153; debriefing report No 9962 and debriefing report No 10217.

[74] Debriefing report No 10217.

[75] Debriefing report No 10771.

The EDPS considers that such detailed information reveals a combination of distinguishing features about an individual that would be sufficient to render those individuals identifiable. It is not necessary to establish that Frontex itself be in a position to identify an individual from this information in order to classify the information as personal data. Identification may take place, for instance, should a security breach occur leading to an accidental or unlawful disclosure of debriefing reports into the public domain. Such an incident could, as in the example of the above-mentioned [redacted] national, have grave consequences for the interviewee. This is why the processing of information defined as personal data within the meaning of data protection law triggers the obligation of the controller to implement the set of standards and safeguards laid down in data protection law (e.g. security standards, access controls, retention periods) in order to minimise the risks associated with the processing and protect the data subject from interferences with his or her fundamental rights.

EDPS assessment of the likelihood of indirect identification of the interviewee via additional information

Further to the considerations above, the audit team assessed the extent to which an interviewee may be indirectly identifiable through Frontex' access to additional sources of information.

The Court has confirmed that the use by the EU legislator of the word "*indirectly"* in Article 3(1) of Regulation 2018/1725 suggests that in order to treat information as "personal data", it is not necessary that the information alone allows the data subject to be identified,[76] but that consideration should be given to whether additional information exists which could be used to identify the data subject, and whether there are means of obtaining that additional information which are reasonably likely to be used.

According to Article 3(6) of Regulation 2018/1725, 'pseudonymisation' means 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

The difference between pseudonymised personal data and anonymous data is therefore that in the case of anonymous data, there is no 'additional information' that can be used to attribute the data to a specific

[76] ECJ Judgment in *Breyer*, C-582/14, ECLI:EU:C:2016:779, para 41.

data subject, while in the case of personal data which has undergone the process of pseudonymisation, there is such additional information. Therefore, in order to assess whether data are anonymous or pseudonymised, one needs to consider if there is any 'additional information' that can be used to link the data to the data subject.

[redacted]."[77] It therefore appears that in cases where an individual has submitted (or intends to submit) a complaint concerning a fundamental rights violation, for instance via the Frontex Complaints Mechanism, which would include information directly identifying the individual concerned, the DO is required to explain to the individual during the debriefing interview that inclusion of their testimony describing the incident in the debriefing report could undermine the anonymity of that report.

The EDPS considers that in such cases, as described by the Handbook to the Operational Plan, the debriefing reports concerned by this scenario would contain pseudonymised personal data.

The EDPS further notes that additional information which could be used to identify an interviewee may be held by another party in the context of Joint Operations: the host Member State authorities.

Recital 16 of Regulation 2018/1725 states that in order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly.

Thus it is not required that all the information enabling the identification of the data subject must be in the hands of one entity.[78]

The EDPS notes that debriefing interviews take place in the context of a wider system of reception and processing of intercepted third country nationals, which includes the registration and screening of those persons by Member State authorities, and to which Frontex participates actively in the context of Joint Operations (see section 4.1.4.2 on controllership).

[77] Handbook on the Operational Plan, p.10.

[78] See also Breyer, para 43.

Screening interviews are aimed at establishing the nationality of the interviewee and in doing so/or as an additional objective, can focus on collecting information related to place of origin, routes, migration methods, and other modus operandi.[79]

Consequently, there may be screening reports which identify interviewees, and include detailed information on that individual, available to Member State authorities; and debriefing reports containing overlapping/duplicating information, which do not name the interviewee, and are available to both the Member State and Frontex. It appears possible therefore that additional information held by Member State authorities, including in screening reports, if compared against information held in debriefing reports, could enable the identification of the subject of the debriefing report.

Assessing whether the means of identification through use of additional information from a third party is "reasonably likely to be used", requires taking into account all objective factors, such as the costs of and the amount of time required for identification.[80] The EDPS notes the threshold set by the Court for qualifying an outcome as "reasonably likely" in this context as excluding cases where "the identification of the data subject is prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, costs and man-power, so that the risk of identification appears in reality to be insignificant."[81]

In the case at hand, the very close cooperation between Member State authorities and Frontex teams in the context of Joint Operations, and their relationship as joint controllers for debriefing interviews (see section 4.1.4.2 below), indicates that a disproportionate effort would not be required in practice for authorities to link information and re-identify individuals concerned, should they so wish.

Conclusions

In light of the considerations outlined above, the EDPS considers that merely excluding the name of the interviewee is insufficient to consider the information included in debriefing reports as anonymous data within the meaning of data protection law. The interpretation of anonymisation in accordance with Recital 16 of Regulation 2018/1725 is one in which anonymisation renders the data subject no longer identifiable, i.e. the

[79] Minutes of the audit, pp. 6-7.
[80] Recital 16 Regulation 2018/1725.
[81] Breyer, para 46.

processing irreversibly prevents identification.[82] The EDPS finds that in the case of debriefing reports the possibility of re-identification cannot be fully excluded.

The EDPS thus finds that debriefing reports should be considered as containing personal data concerning the interviewee and should be handled in accordance with the relevant requirements laid down in the EBCG Regulation and Regulation 2018/1725.

While the EDPS acknowledges that the EBCG Regulation does, in principle, provide Frontex with the legal basis to process personal data concerning migrants for the purpose of risk analysis under Article 88(1)(a), the EDPS strongly welcomes the decision by Frontex not to include direct identifying information, such as the name of the interviewee, in debriefing reports. The EDPS considers that this safeguard significantly reduces the risk of identification of the individuals concerned, and is in accordance with the data minimisation principle, and with Article 88(2)(c) which provides for the processing of personal data of persons who cross an external border without authorisation for risk analysis only insofar as this is necessary for that purpose. Consequently, the EDPS underlines that this safeguard should be maintained.

Further, and in light of the fact that some reports will include personal data which has undergone the process of pseudonymisation, i.e. only allowing for the identification of the interviewee when combined with additional information, the EDPS considers that this information should be subject to organisational and technical measures, to ensure that personal data cannot, through the use of additional information, be attributed to an identified or identifiable natural person, in accordance with the definition of pseudonymised personal data laid down in Article 3(6) of Regulation 2018/1725.

This is particularly necessary, as the EDPS audit team has seen no evidence of an arrangement between Frontex and Member State authorities, providing for rules and safeguards to prevent exchange and/or comparison of information which could identify interviewees.

Finding 3	Frontex includes in debriefing reports personal data about persons suspected of involvement in cross-border crime collected from debriefing interviewees.
Finding 4	Personal data about persons suspected of involvement in cross-border crime [redacted]

[82] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216).

	[redacted] in order to ease the redaction process, before the debriefing report is shared with operational analysts in the Risk Analysis Unit.
Finding 5	Information contained in some debriefing reports concerning interviewees (third country nationals not suspected of involvement in cross-border crime) constitutes personal data within the meaning of data protection law.

Recommendations

In light of the EDPS' assessment that the information included in debriefing reports will, in many instances, constitute personal data, and because the obligations laid down in Regulation 2018/1725 and the data protection provisions of the EBCG Regulation will therefore apply to this data, the EDPS deems necessary that Frontex:

Recommendation 2	Conduct a thorough reassessment of its procedures for processing debriefing reports and implements the necessary measures to ensure compliance with the full set of data protection requirements provided by Regulation 2018/1725 and by the EBCG Regulation.
Deadline	Six months following receipt of this report

In order to ensure adequate pseudonymisation of the personal data included in debriefing reports concerning the interviewee, in accordance with the definition laid down in Article 3(6), the EDPS deems necessary that Frontex:

Recommendation 3	Establish, with respect to the phase of the data processing which consists in the collection of personal data via the debriefing interviews, a clear set of rules prohibiting the sharing of information originating from different stages of migrant reception and processing (registration, screening and debriefing). Such rules could be included, for instance, in the Joint Controllership Arrangement to be established with Member States (see recommendation 4).
Deadline	Six months following receipt of this report

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendations **within the specified deadlines**.

D) INTELLIGENCE REPORTS

[redacted][83] Frontex has not implemented nor used intelligence reports so far, not even in a pilot project. The process for handling these reports would be the same as for the Debriefing reports. [redacted].[84]

Frontex states that it has not yet implemented or used intelligence reports as an additional source of data collection on "suspects" of cross-border crime. The EDPS did not find any evidence to the contrary.

4.1.4.2. Controllership

A) IDENTIFICATION OF THE ROLE OF FRONTEX AND OF THE MEMBER STATES' COMPETENT AUTHORITIES

In this section the EDPS assesses the role of Frontex and of the Member States' competent authorities regarding the phase of the data processing which consists in the collection of personal data via the debriefing interviews. The correct allocation of roles to the different parties to the processing is of utmost importance as this implies different responsibilities for each party (the controller is responsible for ensuring compliance with the data protection legal framework while the role of the processor is limited in line with Article 29 and 87 of Regulation 2018/1725).

Debriefing interviews of migrants are conducted in the framework of Joint Operations carried out in Member States. Frontex may launch a Joint Operation upon a request from a Member State.[85] It can also recommend a

[83] See section 15.8 of the Handbook to the Operational plan.
[84] Minutes, p.8
[85] Article 37 of Frontex Regulation.

Joint Operation to a Member State based on the results of its vulnerability assessment or risk analysis.[86]

All Joint Operations are set up in agreement with the host Member State (i.e. the Member State in which or from which a Joint Operation is launched)[87] and based on an Operational Plan. The Operational Plan defines the aim of each Joint Operation. It covers all aspects considered necessary for carrying out the Joint Operation including a description of the tasks and data protection requirements.[88]

During Joint Operations, Frontex's DO interview irregular migrants to collect information [redacted]

The audit activities have shown that the DO-DBRs can be tasked by both the Member State (i.e. the Team leader) and Frontex's headquarters and that they together (Member States and Frontex) agree on the intelligence gaps to be filled in via the debriefing interviews. In addition, operational analysts provide weekly and monthly reports containing intelligence that DO-DBRs can consult/read.[89]

Moreover, the review of the relevant documentation indicates that:

- the Operational Plan[90]:
    - states that with regard to the data processing conditions for operational personal data under Article 90 of EBCG Regulation, it has been agreed with the Member States[91] and with the EDPS that "*the controller of the personal data is the host MS"*;

[86] Article 41 of Frontex Regulation.
[87] Article 2(20) of Frontex Regulation.
[88] Article 38 (3) of Frontex Regulation.
[89] Refer to audit minutes, p. 14.
[90] General plan Multipurpose operational activities in the Member State (MOA-MS), version of 24.01.22, p. 55 - 56.
[91] In the Frontex Management Board Decision 58/2015.

- anticipates that this may change with the amendment of the Management Board Implementing Rules and in line with subsequent opinions of the EDPS on new processing activities regarding operational personal data;
- mentions that specific conditions may be further defined in the corresponding Specific Activity Plan depending on the types of operational activities to be developed; those conditions aim at identifying the parties responsible for compliance with data protection, as well as at the identification of the specific legal framework covering the specific processing activities;

- Partially in line with the above, the Specific Activity Plans reviewed provide for more specific conditions regarding the operational activity of debriefing interviews and consider the Member States' competent authorities and Frontex as joint controllers for collecting personal data related to suspects of cross–border crime through debriefing interviews.[92]

Article 3(8) of Regulation 2018/1725 defines a "controller" as "(…) the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law". This definition is essentially **functional**: the entity that decides on the "why" and the "how" of the processing will be the controller, independently of its organisational status.[93]

Article 28 of Regulation 2018/1725 defines that "where two or more controllers or one or more controllers together with one or more controllers other than Union institutions and bodies jointly determine the purposes and means of the processing, they shall be joint controllers."

The definition of the controller contains several elements ("Union institution or body or the directorate-general" or "natural or legal person, public authority or other body"; "determines", "alone or jointly with others", "the purposes and means").

"determines"

[92] Specific Activity Plan, Amendment no 3, Joint Operation TERRA 2022, p. 65 - 66, Specific Activity Plan, JO POSEIDON 2022, p. 42 -44.

[93] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 2019 ('EDPS Guidelines'), p. 7. EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2021 ('EDPB Guidelines'), p. 12.

The controller must be the one who “determines” the purpose and the means of the processing and in particular the one who exercises influence over the processing, by virtue of a decision-making power. [94] In case the control is stemming from legal provisions, the law would in principle establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law.

The controller will normally be the one designated by law for the realisation of this purpose. In the absence of control arising from legal provisions, the qualification of a party as controller must be established on the basis of an assessment of the factual circumstances surrounding the processing. All relevant factual circumstances must be taken into account in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question. The need for factual assessment also means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.

“purposes and means”[95]

The determination of “the purposes and the means” of the processing amounts to deciding respectively “why” the processing is taking place (i.e., “to what end” or “what for”) and “how” this objective shall be reached. The controller must decide on both purpose and means of the processing. In case a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. Therefore, a margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. Decisions on the purpose of the processing are clearly always for the controller to make. As regards the determination of means, a distinction can be made between essential and non-essential means. “Essential means” are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. Examples of essential means are the type of personal data, which is processed, the duration of the processing, the categories of recipients and the categories of data

[94] EDPS Guidelines p. 8. EDPB Guidelines 07/2020, p. 11-13.
[95] EDPS Guidelines, p. 9-10. EDPB Guidelines 07/2020, p. 14-16.

subjects. “Non- essential means” concern more practical aspects of implementation, such as the choice of a particular type of hardware or software or the detailed security measures which may be left to the processor to decide on.

“alone or jointly”

The qualification as joint controllers may arise where more than one actor is involved in the processing. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue. Joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities regarding the purposes and essential means.

In more detail, as regards the requirement of “jointly determined purpose”, this can be the case that the entities involved process the data for the same, or common, purposes. However, even when the entities do not have the same purpose for the processing, joint controllership may also be established when the entities involved pursue purposes, which are closely linked or complementary. [96]

Regarding the requirement of “jointly determined means”, joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing. [97]

---

[96] ECJ Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 34 - 39, EDPS Guidelines, p. 23, EDPB Guidelines, p. 20-21.

[97] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraphs 68, 71, 77-79. EDPB Guidelines, p. 21-23.

In the case under consideration and in so far as the phase of the data processing which consists in the collection of personal data via the debriefing interviews is concerned, the EDPS considers that the host Member State and Frontex are joint controllers as they both jointly define the purpose and the means of the processing. The EDPS has previously assessed under the legal framework in force in 2015[98] and 2016 [99] and based on the information conveyed by Frontex on how debriefing interviews were then conducted that "*the host Member State [is] the controller of the debriefing operations*"[100]. However, the changes in the legal framework as well as the audit activities impose that this assessment is updated.

With regard to the purpose of the processing it has to be noted that both parties pursue closely related objectives. In particular, Frontex processes operational personal data in order to perform its tasks under Article 90 of the EBCG Regulation, i.e. to identify suspects of cross border crime and to exchange these data with Europol, Eurojust and the competent law enforcement authorities of the Member States while the host Member State's competent law enforcement authorities process operational personal data collected via debriefing interviews for the prevention, detection, investigation or prosecution of serious cross-border crime.

With regard to the means of the processing, Frontex and the host Member States' competent law enforcement authorities jointly decide on the essential means such as the operational personal data to be processed and the data subjects to be interviewed (through the common identification of intelligence gaps to be filled in via the debriefing interviews as described in the beginning of this chapter) while other essential means are provided for directly by law (such as the retention period, which is defined in Article 91 of the EBCG Regulation and in the criminal proceedings code of the host Member State).

The same considerations are valid for the collection of personal data of interviewees (i.e. personal data not processed under Article 90 of the EBCG Regulation). The EDPS considers that the host Member State and

[98] Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25.11.2004, p. 1–11.

[99] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, OJ L 251, 16.9.2016, p. 1–76

[100] Opinion on the Update of the notification for prior checking opinion received from the Data Protection Office of Frontex of 24 November 2016 and Opinion on a notification for Prior Checking received from the Data Protection Officer of 3 July 2015.

Frontex are joint controllers as they both jointly define the purpose and the means of the processing. The common purpose pursued with the collection of personal data of interviewees via debriefing interviews is conducting risk analysis based on the information collected, such as information on push and pull factors, on smuggling networks and on their modus operandi. With regard to the means of the processing, Frontex and the host Member States' competent authorities jointly decide on the essential means such as the personal data to be processed and the data subjects (through the common identification of intelligence gaps to be filled in via the debriefing interviews).

b) Arrangement between joint controllers

Joint controllers have to enter into a specific arrangement, laying down their roles and responsibilities, in particular towards the data subjects. With regard to operational personal data, this is an obligation under Article 86 of Regulation 2018/1725, while with regard to non-operational personal data the obligation stems from Article 28 of the same Regulation, unless and insofar a law already determines these roles and responsibilities.

The arrangement should at least provide for the following points[101]:

- The respective responsibilities, roles and relationships, so that the lawfulness, fairness and proportionality of the processing operations in place may be identified;
- The respective duties of the joint controllers to provide information referred to in Article 79 of Regulation 2018/1725;
- The responsibilities for information security, including the reporting of personal data breaches;
- A contact point for data subjects requests;
- Cooperation between joint controllers for the reply to data subjects requests and as regards the exercise of other rights of the data subjects;
- Cooperation between joint controllers when carrying out Data Protection Impact Assessment ("DPIA");
- Possible processor(s) engaged by one (or more) of the joint controllers.

Furthermore, according to Articles 86(2) and 28(2) of Regulation 2018/1725, the arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and the

[101] EDPS Guidelines p. 28-29 providing guidance on Article 28 Regulation (EU) 2018/1725, which is the equivalent for non-operational personal data.

essence of the arrangement shall be made available to them. This provision underlines the importance of identifying the roles and responsibilities between joint controllers in order for data subjects to be able to understand clearly the division of responsibilities and whom to address first. This information should be made available to data subjects via the data protection notice.[102]

The review of the relevant documentation and of Frontex's website revealed that the allocation of the roles and the responsibilities between Frontex and Member States' competent authorities only partially takes place with regard to operational data in the Operational Plan[103] and in the Specific Activity Plans ("SAPs")[104]. In particular:

- The Operational Plan[105] provides that specific conditions may be further defined in the corresponding SAPs depending on the types of operational activities to be developed. Those conditions will aim at identifying the responsible parties for compliance with data protection, as well as at the identification of the specific legal framework covering the specific processing activities.
- Frontex undertakes the obligation to ensure transparency via the appropriate notice and record for operational personal data related to suspects of cross-border crime received from the host Member State.[106]
- The data protection notice available online in Frontex' website[107] regarding the processing of personal data for risk analysis (PeDRA) does not cover the phase of the data processing which consists in the collection of operational personal data via debriefing interviews. The data protection notice, which was drafted under the previous legal framework[108], considers Frontex (and in particular the Head of the Risk Analysis Unit (RAU)) as the sole controller for the processing operations taking place as of the moment that Frontex receives the operational data from the Member States.

---

[102] EDPS Guidelines p. 29-30.

[103] General plan Multipurpose operational activities in the Member State (MOA-MS), version of 24.01.22, p. 55 - 60.

[104] Specific Activity Plan, Amendment no 3, Joint Operation TERRA 2022, p. 65 - 66, Specific Activity Plan, JO POSEIDON 2022, p. 42 -44.

[105] General plan Multipurpose operational activities in the Member State (MOA-MS), version of 24.01.22, point 13.1, p. 56.

[106] General plan Multipurpose operational activities in the Member State (MOA-MS), version of 24.01.22, point 13.2.1, p. 56.

[107] Available under https://frontex.europa.eu/assets/Data_Protection/Privacy_Statement.pdf .

[108] Regulation (EU) 2016/1624 of the European parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC.

- With regard to the accuracy of operational personal data, the host MS will strive to communicate to Frontex those cases where data may not have been accurate. In particular, the host MS will communicate to Frontex when there are no longer reasonable grounds to suspect that an individual has been involved in cross-border crime. In those cases, Frontex will delete the data immediately.[109]
- The host MS takes the responsibility of ensuring appropriate technical and organisational measures for all the personal data processed within an operational activity. In case of a personal data breach, the host MS will notify the occurrence of such breach to their National Data Protection Authority and communicate the breach to Frontex. In relation to the operational personal data allowed to be processed by Frontex, Frontex shall notify possible data breaches to the European Data Protection Supervisor and communicate those to the host MS.[110]

Moreover, even this partial allocation of the roles and the responsibilities is not made available to the data subjects.

Regarding the processing of personal data of migrants, there is no allocation of roles and responsibilities between Frontex and the Member States' competent authorities. This is due to Frontex erroneously (see above section.4.1.4.1 c)) considering that the debriefing reports do not contain information directly identifying the interviewees, thus assuming that the information about interviewees contained in these reports is anonymous and that, as a consequence, there is no processing of personal data.

Finding 6	For the phase of the data processing which consists in the collection of operational personal data via the debriefing interviews, the host Member State's competent authorities and Frontex are joint controllers within the meaning of Article 28 and Article 86 of Regulation 2018/1725.
Finding 7	The existing arrangement between the joint controllers for the allocation of their respective data protection obligations in line with Article 86 of Regulation 2018/1725 included in the

[109] General plan Multipurpose operational activities in the Member State (MOA-MS), version of 24.01.22, point 13.2.4, p. 57.

[110] General plan Multipurpose operational activities in the Member State (MOA-MS), version of 24.01.22, point 13.2.6, p. 57.

	Operational Plan and in the Specific Activity Plans is not complete.
Finding 8	There exists no arrangement between the joint controllers for the allocation of their respective data protection obligations in line with Article 28 of Regulation 2018/1725 regarding the processing of personal data of migrants.
Finding 9	The essence of the joint controllers' arrangements is not available to the data subjects as required by Articles 28 (2) and 86 (2) of Regulation 2018/1725.

Recommendations

In order to ensure compliance with Articles 86 and 28 of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 4	Complement the joint controllers' arrangement in line with Article 86 Regulation 2018/1725
Deadline	Six months following receipt of this report
Recommendation 5	Conclude an arrangement in line with Article 28 Regulation 2018/1725 with the host Member State's competent authorities regarding the processing of personal data of migrants.
Deadline	Six months following receipt of this report
Recommendation 6	Make the essence of the joint controllers' arrangements available to the data subjects as required by Articles 28 (2) and 86 (2) of Regulation 2018/1725..
Deadline	Six months following receipt of this report

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendations **within the specified deadlines.**

4.1.4.3. Fairness of the collection of personal data through debriefing interviews

A) Principle of fairness under Regulation 2018/1725

Fairness constitutes a general principle of data protection law, enshrined in Article 8(2) of the EU Charter. The requirement for Frontex to process

data fairly is a specific legal obligation under Articles 4(1)(a) and 71(1)(a) of Regulation 2018/1725 (according to whether personal data is processed for purposes of migration management or for the purpose of identifying suspects of cross-border crime in order to facilitate information exchange with the law enforcement authorities of MS, Europol and Eurojust).

The principle of fair processing requires that there is a clear understanding on the part of the individuals concerned of the way in which personal data collected from them will be used and the impacts of that processing.[111] Fairness obliges openness on the part on the controller to ensure that processing does not exceed the reasonable expectations of data subjects; it manifestly excludes deception or misleading of individuals at the moment of data collection.[112]

Fairness also imposes obligations beyond transparency requirements.[113] In order to comply with the obligation of fair processing, assessment should be made of how the processing will affect the interests and fundamental rights of those concerned, as a group and individually, and personal data should not be used in ways that could have unjustified adverse effects on them.[114] The fairness principle underpins requirements for procedural safeguards as regards the collection and processing of data as well as the exercise of balancing rights and interests under the data protection framework, as reflected in the case law of the Court of Justice of the European Union ("CJEU") and the European Court of Human Rights ("ECtHR"). [115] Consequently, the fairness principle plays an implicit role in the protection of individuals from controller overreach and has an overarching purpose to counter power asymmetries in the data subject-controller relationship, particularly in situations of data subject vulnerability.[116]

---

[111] See Recitals 20 and 35 of Regulation 2018/1725 which evidence the close link between fair processing, transparency and information provision. See also Article 15(2) of Regulation 2018/1725.

[112] Refer to EDPS (2019), "Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation," pp.11-12; see also EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, pp.17-19.

[113] Openness on the part of a controller does not negate the fact that other contextual factors, such as the inherent power imbalance in controller-data subject relationship, may impede an individual from exercising a fully autonomous choice in practice.

[114] Paragraph 12 of the EDPB Guidelines 2/2019; see also Information Commissioner's Office: Guide to the GDPR.

[115] See: College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer [2009] Court of Justice of the European Union C-553/07. and X [2013] Court of Justice of the European Union C-486/12; in relation to the balancing of different fundamental rights see Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014] Court of Justice of the European Union C-131/12; Promusicae v Telefónica [2008] Court of Justice of the EU C-275/06, Curia.

The obligation for fair processing as outlined above takes on a specific meaning within the context of data collection for law enforcement purposes. Under Article 71(1)(a) of Regulation 2018/1725, fairness is ensured not only by procedural safeguards included in the data protection legal framework, but also by those laid down in criminal procedural law, including provisions to protect the presumption of innocence, right to a fair trial, and the right to remain silent and not to incriminate oneself.

B) ASSESSMENT OF THE FAIRNESS OF DATA COLLECTION IN THE CONTEXT OF DEBRIEFING INTERVIEWS

The EDPS considers that the debriefing interview exercise carries the risk of adverse consequences for the individuals concerned by the data collection. Debriefing interviews imply high risks for third parties reported as suspects involved in cross-border crime, should that information prove unreliable or inaccurate. They also imply risks for the interviewee, should individuals face reprisals from facilitators or smugglers or should migrants incriminate themselves during the interview. [redacted]

The EDPS finds that the nature of the debriefing interview, even if not directly targeted at obtaining information about the interviewee, by targeting the collection of information on migratory routes and incidentally related serious crimes, puts the interviewee at risk of self -incrimination, putting at risk in the same vein the presumption of innocence, the right to a fair trial and their right to remain silent.[117] The safeguard put in place to tackle this risk [redacted].[118] However, as outlined further below, the EDPS finds this safeguard insufficient to protect the interviewee's right to remain silent.

Taking into account that debriefing interviews can give rise to collection of personal data, not only of third parties but also of interviewees, [redacted] the EDPS, in light of the considerations above, makes the following observations concerning the conduct of debriefing interviews as

[116] See paragraph 12 of the EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects; Refer also to D. Clifford and J. Ausloos, (2018), Data Protection and the Role of Fairness, Yearbook of European Law, Vol.37, No.1, pp.13-187.

[117] For instance, one of the debriefing reports verified by the audit team included testimony from a Syrian interviewee detailing his involvement with ISIL in his country of origin (cited as a 'push factor' for departure).

[118] Minutes of the audit, pp. 7, 13.

an instrument of data collection, and their compliance with the fairness principle:

Vulnerability of individuals subject to debriefing interview

The EDPS finds that the debriefing interviews, conducted with individuals who are in a position of vulnerability, are potentially very sensitive. While specific categories of individuals are explicitly singled out by Frontex as 'vulnerable' and therefore excluded from potential interview (minors, persons showing evident signs of mental illness),[119] various other factors place persons subject to debriefing interviews in a position of vulnerability. These include the traumatic experience of often lengthy journeys to the EU borders; the uncertainty of their future (potentially subject to asylum or return procedures); their status having been apprehended and detained by border or police authorities; lack of familiarity with the host Member State's legal procedures, processes, and their rights; as well as further intervening factors relating to gender, age, and other personal characteristics. The EDPS is concerned that insufficient consideration may be given to the psycho-physical condition of migrants when selecting potential interviewees ([redacted]).[120]

Presence of appropriate procedural safeguards

The vulnerability of persons interviewed, and the potential severe risks implied by the data collection, places increased importance on the obligation for controllers to establish, and comply with, strong procedural safeguards. Despite this, the EDPS understands that the debriefing interviews are not subject to strict procedural rules. The EBCG Regulation does not explicitly provide for any guidance in this respect, which the EDPS finds in itself sub-optimal. The Frontex Handbook to the Operational Plan makes only a general reference, in relation to debriefing interviews, to the need to follow the rules and procedures in accordance with the legislation of the host country,[121] despite the fact that applicable national rules and international standards relating inter alia to the treatment of detainees[122] should be clearly detailed in internal arrangements and taken

[119] Handbook, p.9.

[120] Minutes of the audit, pp. 10, 11, 14.

[121] Handbook, p.11.

[122] Including relevant standards laid down in the following instruments: UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171; UN Human Rights Committee (HRC), General comment no. 35, Article 9 (Liberty and security of person), 16 December 2014, CCPR/C/GC/35; UN General Assembly, Body of Principles for the Protection of All

into careful consideration during the design and preparation of operational activities.

Where persons subject to debriefing interviews have been deprived of their liberty, whether this is formally referred to as a situation of immigration detention[123] or occurs as de facto detention,[124] they are entitled to minimum standards and procedural guarantees. These include the obligation not to take undue advantage of the situation of a detained or imprisoned person for the purpose of compelling him/her to confess, to incriminate him/herself otherwise or to testify against any other person.[125] Safeguards also include access to the assistance of an interpreter.[126] While the presence of an interpreter is part of the formal procedure of debriefing interviews, the EDPS notes with concern reports concerning the use by Member State authorities of non-professional interpreters/cultural mediators to support debriefing activities - reportedly, in certain cases, other migrants.[127]

In addition, there appears to be no external oversight to monitor the conduct of interviews and ensure compliance with applicable national and international standards, in particular those related to situation of detention and treatment of persons whose liberty is limited or deprived.[128] The

Persons under Any Form of Detention or Imprisonment: resolution/adopted by the General Assembly, 9 December 1988, A/RES/43/173.

123 Understood as the deprivation of liberty for reasons related to a person's migration status. Refer to CMW, General Comment No. 5 on Migrants' Rights to Liberty, Freedom from Arbitrary Detention and Their Connection with Other Human Rights, CMW/C/GC/5, (September 23, 2021), para. 15. UNHCR, APT, and IDC refer to immigration detention as "the deprivation of an individual's liberty, usually of an administrative character, for an alleged breach of the conditions of entry, stay or residence in the receiving country," see UNHCR, Association for the Prevention of Torture (APT), and International Detention Coalition, Monitoring Immigration Detention: Practical Manual, 2014, p. 20.

124 Measures which in practice amount to a deprivation of liberty but which states do not formally qualify as such. The CJEU and the ECtHR, in qualifying a deprivation of liberty, place an emphasis on whether persons are allowed to leave the premises and on the levels of restriction of movement. Refer for instance to: ECtHR, J.R. and Others v. Greece, 22696/16, (January 25, 2018), para. 86; ECtHR, Khlaifia and Others v. Italy, 16483/12, GC, (December 15, 2016), para. 65-72; CJEU Joined Cases C-924/19 PPU and C-925/19 PPU FMS and Others v Országos Idegenrendészeti Főigazgatóság Délalföldi Regionális Igazgatóság and Országos Idegenrendészeti Főigazgatóság [2020].

125 Principles of Detention or Imprisonment, principle 21(1); ICCPR, Article 14(3)(g).

126 WGAD, Revised Deliberation No. 5 on deprivation of liberty of migrants, para. 35; see also: https://rm.coe.int/16806cce8e

127 Minutes of the audit, p.32.

128 Refer to the obligation for a monitoring system to apply to all detention facilities for migrants. See for instance, Parliamentary Assembly of the Council of Europe, Resolution n. 1637 (2008), op. cit., para. 9.14.

Fundamental Rights Monitors interviewed by the EDPS reported that they were prevented from observing debriefing interviews.

EDPS further recalls that persons within the criminal justice process (witnesses or victims) are entitled to a number of procedural rights and safeguards, including the right to legal advice, information, and additional forms of support. Suspects and accused persons are accorded the right to remain silent, an important aspect of the presumption of innocence which serves as protection from self-incrimination.[129] The right to remain silent also includes the right not to be forced, when asked to make statements or answer questions, to produce evidence or documents which may lead to self-incrimination. Under EU law, suspects and accused persons are accorded the right to interpretation and translation,[130] to access a lawyer, and to communicate with consular authorities when deprived of their liberty.[131]

The EDPS notes that it is not the primary purpose of debriefing interviews to incriminate or otherwise lead to any adverse legal effects on the interviewee, despite the fact that self-incrimination can occur. As such, they are not identical to a situation of interrogation of a suspect, in the criminal law meaning of this word. At the same time, however, as already underlined above, these interviews are (1) conducted in the situation of deprivation (or limitation) of liberty, (2) aimed at identifying suspects among people known to the interviewee on the basis of her/his testimony. Moreover, they might, in case of self-incriminating testimonies, put the interviewee under the relevant national procedures.

The EDPS notes in this regard, the observations and recommendations of the Spanish Ombudsman stemming from its investigation into the conduct of debriefing interviews in Spain, which identify a failure to respect the procedural safeguards laid down in the Spanish constitution and Spanish criminal procedural law.[132]

---

[129] Refer for instance to Directive (EU) 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65/1.

[130] Directive (EU) 2010/64/EU of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ L 280/1.

[131] Directive (EU) 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294/1.

[132] Namely, Article 17.3 of the Spanish Constitution and Article 520 and following of the Criminal Procedure Law. The Spanish Ombudsman also issued observations and recommendations related to the vulnerability of interviewees, non-voluntary nature of the interviews, in addition to the lack of legal guarantees: Defensor del Pueblo, Decision on Frontex Operational Plans in Spain,

The EDPS is therefore of the opinion that from the point of view of legal certainty, the organisation of debriefing interviews require the specification of the EU or national laws or international standards that determine the norms by which the interviews need to be held (i.e. type of information provided to the interviewee, length, considerations for vulnerable people, recourse to possible assistance etc.).

As a result, the EDPS concludes that more specific procedural safeguards accompanying the debriefing interviews should be developed.

Informed and voluntary nature of the debriefing interview

The lack of legal guarantees and procedural safeguards cannot be mitigated by the contention that debriefing interviews are voluntary. The EDPS finds that the circumstances in which they are conducted and the very specific situation of persons interviewed makes it difficult for the informed and voluntary nature of the interviews to be ensured.

In particular, the EDPS questions whether interviewees are always fully aware of the nature, purpose and full implications of the interview and whether the subsequent handling of the data collected meets their reasonable expectations. [redacted] - is not coherent with the obligation to ensure that individuals can make a fully informed, autonomous choice, and may be construed as a means to exploit a lack of awareness on the part of interviewees.

While the EDPS acknowledges that Frontex DOs are provided with specific trainings,[134] and subject to guidance directing them to provide adequate information about the purpose and voluntary nature of the interview, information provision is limited to a verbal exchange, and given the lack of

https://www.defensordelpueblo.es/resoluciones/planes-operativos-de-las-actuaciones-de-frontex-en-espana/

[133] The Handbook to the Operational Plan (p.8) states: “In this way migrants do not have the opportunity to first converse with others and decide to provide a false account but are more likely to give a truthful account. Once newly arrived migrants integrate with others in the detention centre, there is a tendency for them to become more reluctant to cooperate and provide any information during the interview process.”

[134] Minutes from the audit, p. 15.

records or oversight,[135] cannot be subject to monitoring or verification. The EDPS notes with concern reports of Team Leaders encouraging Frontex Debriefing Officers to promise the migrants potential benefits in return for their testimonies.[136]

[redacted]"[137] While the EDPS acknowledges that the intention is to build trust through a friendly, informal exchange, this approach does not facilitate transparency. The interview is very much part of the official screening and registration process, the Debriefing Officers are working in tandem with local authorities, the information collected will be shared with those authorities by default (reports sent via the Intelligence Officer and Member State Reader) and [redacted]

The abovementioned circumstances therefore raise the EDPS' concerns that interviewed persons might, among others:

- take the interview out of fear, lack of understanding, not knowing they can refuse,
- take the interview hoping to receive some form of advantage in return,
- not know what is the specific role of Frontex (including that it is not related to any asylum procedures),
- not know that their testimony might lead to processing of personal data of persons mentioned by them in Europol's databases,
- not know that their testimony may result in self-incrimination and immediate referral to the national competent authority,
- face potential consequences for talking to Frontex officers from other individuals detained in the camps, as the fact they take the interview might be known to other migrants and perceived negatively (i.e. if following the interviews, migrants who are pointed as smugglers of facilitators are subsequently detained by the authorities).

---

[135] Minutes of the audit, p.14; and pp.32-33.

[136] In reply to the question on whether the nature of the debriefing interview is in his/her view clear to the migrant, FROM informed that she/he cannot be certain about it. FROM recalled a situation where a team leader explicitly instructed debriefing officers to encourage migrants to take part in the debriefing interviews by offering them potential benefits or positive outcomes in return. Minutes of the audit, p. 33.

[137] Handbook, p. 11.

In light of the vulnerable position of the interviewee, in particular vis-a-vis the Frontex Debriefing Officer, the EDPS has severe doubts that current arrangements for debriefing interviews guarantee their voluntary nature. This is compounded by reports to the EDPS during the audit of debriefing interviews that were described as unpleasant and "rough".[138] In one situation, the mobile phone of the migrant was taken and photos from the phone were searched and shown to contest the statements made by the migrant.[139]

Conclusions

In light of the observations above, the EDPS has serious doubts as to whether the conduct of debriefing interviews in their current form is in compliance with the principle of fair processing as required by Articles 4(1)(a) and 71(1)(a) of Regulation 2018/1725. In particular, the activity does not take sufficient account of the high vulnerability of the individuals targeted for data collection, nor ensure that processing implied by the activity is reasonably foreseeable for individuals from whom data is collected. In addition, the EDPS finds that Frontex does not provide for appropriate procedural safeguards that are coherent with the status of interviewees as detainees and the law enforcement nature of the information and personal data provided, and that could protect individuals concerned from adverse and disproportionate risks to their fundamental rights.

The EDPS is aware of the specific role in which Frontex operates, namely as a support to the activities exercised by relevant authorities of the Member States, as provided by the EBCG Regulation and described in the Operational plan and the Specific Activity Plans. This does not however alleviate Frontex from its duty, as an EU agency, to act within its legal framework, which includes also the EU primary law, in particular the Charter of Fundamental Rights as well as international legal obligations, as mandated by Article 80 of the EBCG Regulation and reflected in Frontex' Fundamental Rights Strategy.[140] While a certain dependence of Frontex on Member State's authorities determining the role and involvement of Frontex might pose a limitation, the onus is ultimately on Frontex to ensure it is in a position to engage in activities which do not infringe such legal obligations, especially as Frontex is an equal party to Joint Operations. While it is a joint obligation of Frontex and Member States authorities to ensure full respect for fundamental rights, the EDPS findings

[138] Minutes of the audit, p.33.

[139] Minutes of the audit, p.33.

[140] Fundamental Rights Strategy, endorsed by the Fundamental Rights Officer on 25 January 2021 and adopted by the Management Board on 14 February 2021, Warsaw.

and recommendations, due to its competence, are limited to those applicable to Frontex, as an EU agency.

Finding 10	The vulnerable position of interviewees and the circumstances and manner in which interviews take place means that the voluntary nature of debriefing interviews cannot always be properly ensured
Finding 11	It cannot be verified whether there is a clear understanding on the part of the individual concerned of the way in which personal data collected from them will be used and the impacts of that processing.
Finding 12	Fundamental Right Officer Monitors (FROM) are not, as a general rule, permitted access to debriefing interviews.
Finding 13	It is reported that Member State authorities occasionally use the support of non-professional interpreters/cultural mediators (in some reported cases, other migrants).
Finding 14	The use of personal belongings, in particular of mobile phones, of the interviewed person, is an intrusive measure; the voluntary nature of such searches cannot in every case be ensured.
Finding 15	Debriefing interviews lack adequate procedural safeguards coherent with the extraction of sensitive information (including operational personal data collected to identify suspects of cross-border crime) from persons deprived of their liberty/subject to restrictions on their freedom of movement and in such a vulnerable position.

Findings 10-15 pose a severe risk of non-compliance with Articles 4(1)(a) and 71(1)(a) of Regulation 2018/1725.

The current conduct of debriefing interviews presents risks for the fundamental rights and freedoms of the data subjects. The processing may exceed the reasonable expectations of the data subject, with a potentially severe impact as individuals may be placed in the position of providing self-incriminating information without adequate safeguards. In addition, the processing may result in the interviewee providing inaccurate information on third parties who may later be subject to criminal investigation.

Recommendations

In order to ensure compliance with Articles 4(1)(a) and 71(1)(a) of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 7	Ensure that Fundamental Right Officer Monitors can attend the debriefing interviews. This recommendation should be understood as extending to other type of activities conducted by Frontex at the EU borders, such as screening interviews or patrolling activities, where collection of personal data might take place and where the possibility for the Fundamental Right Officer Monitors to attend is not ensured.
Deadline	Immediately
Recommendation 8	Put in place additional safeguards to ensure that interviews are only conducted with persons in adequate mental and physical condition. This may include laying down a minimum time period for intercepted persons to be adequately assessed and received before undergoing interview.
Deadline	Two months following receipt of this report
Recommendation 9	Take appropriate measures to ensure that in the context of debriefing interviews an access to legal assistance is provided should the person request it, i.e. in order to seek clarification as to the nature of the interview and potential consequences of their statement. Clear information about the nature, purpose and implications of the interview should be provided in a language of the interviewee's understanding, both verbally and in writing.
Deadline	Four months following receipt of this report
Recommendation 10	Specify applicable rules and legislation in a dedicated annex to the Operational Plan/Specific Activity Plan in order to ensure compliance with national procedural requirements when interviewing persons deprived of their liberty/freedom of movement, and with legal guarantees under national criminal procedures.
Deadline	Six months following receipt of this report

Recommendation 11	Ensure that Frontex officers do not take part in debriefing interviews if the support from an interpreter or cultural mediator is not of a professional nature.
Deadline	One month following receipt of this report
Recommendation 12	Make sure that the use of personal belongings in debriefing interviews only takes place (i) when the voluntary nature of the use is strictly ensured and (ii) in compliance with applicable national laws. Applicable rules and legislation should be added to the above-mentioned annex to the Operational Plan/Specific Activity Plan.
Deadline	Six months following receipt of this report

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendations **within the specified deadlines.**

4.1.4.4. Processing of personal data collected from debriefing interviews to identify suspects of cross-border crimes

A) LAWFULNESS PRINCIPLE

Pursuant to Article 72 of Regulation 2018/1725, processing of operational personal data is lawful only if and to the extent that processing is necessary for the performance of a task carried out by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 (Judicial cooperation in criminal matters) or Chapter 5 (Police cooperation) of Title V of Part Three of the Treaty of the Functioning of the European Union ('TFEU').

Under Article 10 (1) (q) of the EBCG Regulation, Frontex is tasked to cooperate with Europol and Eurojust within the respective mandates of the agencies concerned and provide support to Member States in circumstances requiring increased technical and operational assistance at the external borders in the fight against cross-border crime and terrorism. In the performance of this task of cooperation and support, Article 90 of the EBCG Regulation allows Frontex to process personal data that it has collected while monitoring migratory flows, carrying out risk analyses or in the course of operations for the purpose of identifying suspects of cross-border crime. Such personal data must be processed in accordance with Chapter IX of Regulation 2018/1725.

In order to assess whether the collection and further use by Frontex of personal data about suspects of cross-border crime complies with the principle of lawfulness, i.e. whether it has sufficient legal basis in the EBCG Regulation, one must consider the rationale of the establishment of Frontex since its creation in 2004, which is the facilitation of the application of the EU measures relating to the management of the EU external borders.[141] While the tasks of Frontex have been extended to include support to competent EU agencies and national authorities in the fight against cross-border crimes, Article 1 of Frontex's current founding legal act (the EBCG Regulation) states that Frontex is established to ensure European Integrated Border management at EU external borders.[142]

This act is based on Article 77 (2) (b) (d) and 79 (2) (c) of the 'TFEU', which refer to the checks of persons crossing external borders, the establishment of integrated management systems for external borders and illegal immigration. Any activity outside these areas, such as the fight against cross-border crimes, must therefore be considered as secondary and indirectly associated with Frontex. In this regard, and as provided in Article 88 of the TFEU, Recital 41 of the EBCG Regulation recalls that the EU agency responsible for supporting and strengthening Member States' actions and their cooperation in preventing and combating serious crimes affecting two or more Member States is Europol.

The tasks of Frontex are provided in detail in Article 10 of the EBCG Regulation. Conducting debriefing interviews is provided in the context of the migration management support teams deployed at hotspot areas (Article 10 (1) point (m)). This Article read in conjunction with Article 37 (4) and in particular Article 40 of the EBCG Regulation[143] leads to the conclusion that debriefing interviews are part of the migration management tasks of Frontex, such as the risk analysis carried out by Frontex, which is clearly distinct from the prevention of cross-border crimes.[144]

---

[141] Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ, 25.11.2004.

[142] Article 1 EBCG Regulation.

[143] Which, in its para 4, states that "the technical and operational reinforcement provided, with full respect for fundamental rights, by the standing corps in the framework of migration management support teams may include the provision of: (a) assistance, with full respect for fundamental rights, in the screening of third-country nationals arriving at the external borders, including the identification, registration, and debriefing of those third-country nationals (…)".

[144] Article 37(4) EBCG Regulation specifically distinguishes between types of activities related to (1) coast guard functions and the prevention of cross-border crime, and (2) migration management: "The objectives of a joint operation or rapid border intervention may be achieved as part of a multipurpose operation. Such operations

The EDPS interprets Article 90 of the EBCG Regulation read in the light of the provisions defining the Frontex's key role (Article 77 (2) (b) (d) and 79 (2) (c) TFEU and Article 1 of EBCG Regulation) and its tasks (Article 10 of EBCG Regulation) as allowing Frontex to process operational personal data collected only in the context of a specific and lawful purpose, within its mandate, namely - in respect of debriefing interviews - for migration management purposes.

Therefore it is important to note that the objective of the debriefing interviews cannot as such be directed at the gathering of operational personal data. Their primary objective should be in line with Frontex's mandate and separate from the tasks of law enforcement agencies, such as Europol.[145] In other words, while Frontex is entitled to conduct debriefing interviews for migration management tasks, and might - in the course of such interviews - obtain personal data about suspects of cross-border crimes, such collection should not alter the nature of debriefing interviews as migration management tools.

In addition, considering that any activity by Frontex in relation to the prevention, detection and investigation of criminal offences is secondary and should be carried out uniquely as a form of support to Europol, Eurojust and Member States' competent authorities, Frontex may not systematically, proactively and on its own collect any kind of information about suspects of any cross-border crimes. This collection must be strictly limited to identified needs of Europol, Eurojust and MS competent authorities and concerns people (i.e. suspects of cross- border crimes) about whom Europol, Eurojust and MS competent authorities are allowed to process personal data to perform their tasks.

b) Assessment of the lawfulness of the processing

[redacted]

may involve coast guard functions and the prevention of cross-border crime, focusing on the fight against migrant smuggling or trafficking in human beings, and migration management, focusing on identification, registration, debriefing and return."

145 [redacted]

[redacted][146]

The audit activities showed that Frontex conducts debriefing interviews for two purposes:

- identification of suspects of cross-border crime in view of their further transmission to Europol (PeDRA) (processing of operational data) and,
- risk analysis.

The EDPS found no indication of any other type of use of the evidence gathered during the debriefing interviews than the two mentioned above. The EDPS also did not find any indication that operational personal data might be processed outside of PeDRA, namely for the risk analysis purposes as the debriefing interview reports are redacted (i.e. operational personal data are concealed) when used for risk analysis.

At the same time, the EDPS found that Frontex considers both purposes as primary purposes. This is reflected in the Operational Plan and the Specific Activity Plans which mention the tackling of cross-border crimes and law enforcement activities together with other activities such as controlling illegal immigration flows and preventing unauthorised border crossings under the general and specific operational aims of the Joint Operations.[147]

In addition, the EDPS found that debriefing interviews form an activity resulting in the largest operational personal data collection at Frontex. In the period of January 2022 to July 2022, Frontex transmitted 1451 reports to Europol which included 2770 persons suspected of cross-border crimes.[148] Finally, the EDPS found that, currently, debriefing interviews are the only source of operational personal data collected by Frontex.

Finding 16	Operational personal data collected during debriefing interviews are further processed by Frontex only for purposes of (1) transmission to Europol, and of (2) risk analysis. Frontex considers both purposes as primary purposes.

[146] Minutes p.10.

[147] Operational Plan, General plan Multipurpose operational activities in the Member State (MOA-MS), version 14.12.2021, section 4.1, p. 17; SAP JO Poseidon, section 4.1, p.7; SAP JO Terra, section 4.1, p.27; SAP JO Themis, section 4.1, p.10.

[148] Statistics on PeDRA transmissions to Europol for the period of January 2022 to July 2022.

Finding 17	Debriefing interviews form an activity resulting in the largest operational personal data collection at Frontex and currently are the only source of operational personal data collected by Frontex.

Notion of suspect of cross-border crime

The EDPS understands that in the context of debriefing interviews, persons interviewed give testimonies that include personal data of third persons (mostly their names). These, among others, relate to persons who, according to the interviewee, facilitated the journey he or she took.

The EDPS finds that Frontex transmits to Europol in the context of PeDRA all personal data related to these third persons as per the testimony at the debriefing interview. These potentially include data of persons the interviewee has heard of, has seen, but could not verify the credibility of the name given to him/her, or is mentioning under fear or in an attempt to receive some benefits considering his/her highly vulnerable situation (see section 4.1.4.3 above).

The EDPS notes that, with the notion of suspect comes not only an involvement of relevant law enforcement or judicial authorities, but also a certain recognition of procedural rights of a suspect. It is against this background that the notion of suspect is inserted, for example, into the Europol Regulation[149], with Europol being a recipient of data from Member States on suspects. In this regard, Annex II, point A of the Europol Regulation refers to "persons who, pursuant to the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence (...)".

The notion of suspect of a cross-border crime under Article 90 of the EBCG Regulation cannot be considered as *lex specialis* (or bringing alternative meaning) to the framework of the Europol Regulation as Frontex is processing personal data about suspects only in its supporting role to Europol as defined in Article 10 (1) (q) of the EBCG Regulation. Therefore

[149] Regulation 2016/794 of the European Parliament and 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, 24.05.2016, pp. 53-114 as amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ, L 169, 27.6.2022, p. 1–42.

Frontex should not automatically extend the notion of suspect to "any person that is named or mentioned in the course of a debriefing interview", as it currently appears to be the practice.[150] In particular, Article 90 EBCG Regulation requires that the Member States, Europol or Frontex must have reasonable grounds to suspect that an individual is involved in a cross-border crime. A simple reference in a debriefing report cannot, by any means, meet this threshold. The EDPS notes that the European Court of Human rights has considered that suspicions must be justified by verifiable and objective evidence. Vague and general references in the authorities' decisions and documents to a legal provision or unspecified "case material" cannot be regarded as sufficient to justify the "reasonableness" of a suspicion.[151]

The EDPS notes that a validation of the debriefing report before subsequent transmission to Frontex (and then to Europol) is done by the relevant representative of the host Member State. The EDPS understands that such validation should be done in accordance with the threshold defined under the applicable national law. The EDPS could not collect evidence on whether the validation leads to narrowing the number of personal data entries so that the notion of a suspect as per applicable national legislation is ensured as this activity takes place on national grounds.

The Operational Plan and Specific Activity Plans reviewed by the audit team contain no criteria or specific processes about the validation process to be done by the [redacted] of the host Member State. As a result, Europol may be a recipient of data on "suspects" being a sui generis concept contrary to the meaning of this term under EU law. As such, such practice does not meet the criteria of lawfulness by which recipients of data transmitted by Frontex are also bound.

Finding 18	Frontex processes data on persons whose categorisation as suspects is doubtful, as the

[150] Minutes of the audit, p.10-13

[151] *Akgün v. Turkey*, 20 July 2021, application no 19699/18, §§ 156 and 175. The rights of liberty and security of person in Article 6 of the Charter for Fundamental rights of the European Union (the 'Charter') are the rights guaranteed by Article 5 of the European Convention of Human Rights ('ECHR'). In accordance with Article 52(3) of the Charter, they have the same meaning and scope. Consequently, the limitations which may legitimately be imposed on them may not exceed those permitted by the ECHR, in the wording of Article 5. In particular Article 5 §1 c) of the ECHR provides that: 1.Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law: c) the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so".

	criteria to ensure that they meet the threshold of "reasonable grounds" or the ones defined by relevant national laws, as referred to by Europol Regulation, as a recipient of such data from Frontex, are not defined in the respective OPLANs or SAPs.

Recommendation

In order to ensure compliance with Article 72 of Regulation 2018/1725, Articles 10 (1) (q) and 90 of the EBCG Regulation, the EDPS deems necessary that Frontex:

Recommendation 13	Define, for each joint operation, the criteria used to meet the threshold of "reasonable grounds" to qualify a person as suspect of a cross-border crime, in line with the applicable national law. and, Put in place safeguards to ensure that before transmitting operational personal data to Frontex, the [redacted] of the host Member State verifies and validates that personal data contained in the debriefing report only refer to persons for whom there are reasonable grounds to suspect they are involved in cross-border crimes, in line with the applicable national law.
Deadline	Six months following receipt of this report

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendation **within the specified deadline**.

Identified needs of Europol, Eurojust and Member States' competent authorities

As developed above (see point A)), any activity by Frontex in relation to the prevention, detection and investigation of criminal offences is secondary and should be carried out uniquely as a form of support to Europol, Eurojust and Member States' competent authorities.

This implies that Frontex is allowed to act in this area only based on prior targeted requests from Europol, Eurojust and/or MS competent authorities

to support them in the performance of their respective tasks. Frontex may not systematically, proactively and on its own collect any kind of information about suspects of any cross-border crimes. These prior targeted requests are required in order to ensure that the collection of operational personal data does not go beyond Frontex's mandate (Articles 10 (1) (q) and 90 of EBCG Regulation). As developed below (see point D), these requests are also required to comply with Frontex's legal obligation to assess the necessity of the exchange of operational personal data with Europol, Eurojust and/or MS competent law enforcement authorities (Article 90(2) (a) and (b) of the EBCG Regulation).

The EDPS observes that the Specific Activity Plans ("SAPs") are unclear about the types of cross-border crimes in relation to which Frontex may collect personal data through debriefing interviews. [redacted]

The EDPS also observes that SAPs provide background information about trends and criminal activities that have been noticed so far[155], but they do not refer to specific intelligence gaps or ongoing criminal intelligence operations or investigations identified by Member States' competent authorities and/or Europol for which Frontex' support is necessary. Audit activities have revealed that the feedback from Europol is very limited and

[152] SAP Poseidon, section 4.3.8 "Collection of information through debriefing interviews and other operational reports", p. 16.

[153] SAP Poseidon, section 4.2 "Specific operational objectives" p.9

[154] SAP Poseidon, section 13 "Data protection requirements for the joint operations, p.44

[155] See for instance SAP JO Poseidon (p.5) 'Human smuggling networks changed the boat types used for transport migrants, by increasingly utilizing wooden fishing boats. These vessels are not only used for transportation, but also for signalling the presence of coats guards patrols in the area."

is restricted only to [redacted][156]

[redacted][157]

According to Frontex, DOs receive instructions/and or guidelines [redacted].[158] This information seems to rely on the outcome of risk analyses rather than specific needs of support in terms of ongoing criminal [redacted][159]

Finding 19	The Specific Activity Plans are unclear about the cross-border crimes in relation to which Frontex may collect personal data through debriefing interviews nor do they identify intelligence gaps in these areas
Finding 20	[redacted]

Recommendations:

In order to ensure compliance with Article 72 of Regulation 2018/1725, Articles 10 (1) (q) and 90 of the EBCG Regulation, the EDPS deems necessary that Frontex:

Recommendation 14	Ensure that the specific cross-border crimes and the intelligence gaps, for which the

[156] Statistics FRONTEX-EUROPOL transmissions since Jan-2022 (excel sheet) collected as evidence no 12 of Annex 4

[157] For example, SAP JO Poseidon, section 4.3.8, p.16.

[158] See Audit minutes, p. 7, 9, 14 and 15.

[159] See email of 20 October 2022, annex 4, document n°10,, in which it is mentioned that "Frontex's operational analysts discuss any queries on their part in the weekly video conferences with the debriefing teams".

	collection of operational personal data by Frontex through debriefing activities is asked to support MS competent authorities in their fight against cross-border crime and Europol in the performance of its mandate, are clearly identified.
Deadline	Six months following receipt of this report
Recommendation 15	Ensure that Frontex receives specific and targeted requests from Europol prior to the collection of operational personal data and their further transmission to Europol
Deadline	By end of 2023

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendations **within the specified deadlines.**

In order to avoid risks of non-compliance with Article 72 of Regulation 2018/1725, Articles 10 (1) (q) and 90 of the EBCG Regulation, the EDPS recommends that Frontex:

Recommendation 16	Document the instructions transmitted by Frontex's [redacted] to the Debriefing officers

In light of the accountability principle laid down in Article 4 (2) of Regulation 2018/1725, the EDPS expects Frontex to implement the above recommendation accordingly.

C) DATA MINIMISATION PRINCIPLE

Pursuant to Article 71 (1) (c) of Regulation 2018/1725, operational personal data must be adequate, relevant, and not excessive in relation to the purposes for which they are processed.

Article 90 (2) (a) of the EBCG Regulation provides that Frontex will only exchange the operational personal data it has collected while monitoring migratory flows, carrying out risks analysis or in the course of operations with Europol or Eurojust where these data are strictly necessary for the performance of their respective mandates and in accordance with Article 68 of the EBCG Regulation (i.e. within the framework of a working arrangement which is subject to the Commission's prior approval and they are communicated to the European Parliament and the Council).

As stressed by the European Court of Justice, strict necessity must be interpreted as establishing strengthened conditions for the personal data processing.[160] It requires the necessity to be assessed with particular rigour and particular strict checking, in that context, as to whether the principle of the data minimisation is observed.[161]

D) ASSESSMENT OF THE DATA MINIMISATION PRINCIPLE WHEN EXCHANGING OPERATIONAL PERSONAL DATA WITH EUROPOL

[redacted]

The EDPS found that the PeDRA team analysts do not carry out any kind of necessity assessment before sharing the interview report with Europol but they automatically share each and every accepted interview report.[164]

The EDPS considers that pushing all interview reports to Europol does not meet the requirement of data minimisation laid down in Article 71 (1) (c) of Regulation 2018/1725, and thus by extension the requirement of "strict necessity" provided in Article 90 EBCG Regulation.

The EDPS has identified this issue already under the previous legal framework[165] in his Opinion of 3 July 2015 regarding a prior check by Frontex on PeDRA ('Processing of Risk Analysis'), which entailed the

[160] See ECJ Judgment - 26/01/2023 - Ministerstvo na vatreshnite raboti (Biometric and genetic data registration by the police), C-205/21, ECLI:EU:C:2023:49, point 117.

[161] *Idem* points 118 and 125.

[162] See Minutes p. 32 and draft PeDRA intake process, Process description p. 8 which specifies that : " (...) personal data not related to suspects of cross-border crime and terrorism - are rejected during the Legality check and sent back to the MS Intelligence Officer with the request to delete all non-compliant personal data from the interview text and from the entities."

[163] Minutes, p. 25.

[164] Refer to audit minutes, p. 25.

processing of personal data about persons suspected by the Member States' competent authorities to be involved in facilitation of illegal immigration, human trafficking and other cross-border criminal activities including their transfer to Europol.[166]

In this Opinion, the EDPS stressed in particular that personal data should not be pushed on to Europol as a matter of general policy (i.e. pushing all received reports onwards at the latest shortly before they expired as explained in Frontex supporting documents), but only after human intervention and evaluation. It was considered that such transfer should only take place if, based on the information available to Frontex, there is an added value from the connections made between the different reports received and the additional background information provided by Frontex. In this context, the EDPS recommended that Frontex only transfers personal data to Europol when this is necessary and proportionate on a case-by-case basis and defines a methodology for assessing the necessity and proportionality for transfers to Europol.

Following the EDPS' Opinion, the Management Board of Frontex adopted Decision No 58/2015 of 18 December 2015 on implementing measures for processing of personal data collected during Joint Operations, pilot projects and rapid interventions ('MB Decision 58/2015').[167]

The MB Decision 58/2015 includes a specific provision (Article 15) on the transfer of personal data to Europol. This provision lists the legal requirements of any transmission of personal data to Europol. It also requires Frontex to make an evaluation of the necessity and proportionality of the transfer. This evaluation must be based on information supplied in advance by Europol and listed in the Operational Plans.

More precisely, Article 15 of the Management Board Decision 58/2015 provides that the transmission of personal data to Europol must:

- be necessary for the legitimate performance of tasks covered by the competence of Europol (Article 15(1)(a));
- be subject to specific working arrangements (an agreement on the operational cooperation between Frontex and Europol was signed on 4

[165] Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25.11.2004, p. 1–11

[166] EDPS opinion of 3 July 2015 on PeDRA, EDPS Case 2015-346.

[167] MB Decision 58/2015 is still in force to the extent that it does not contradict the provisions EBCG Regulation and considering that the application of MB decision 69/2021 on the processing of operational personal data by Frontex has been suspended.

December 2015 following EDPS' prior approval on 24 March 2015 and is currently under revision[168]) (Article 15(1)(b));
- be on a case-by-case basis (Article 15(1)(d)); and
- respect the principles of necessity and proportionality as regards the purpose of the transmission (Article 15(1)(e)).

In addition, Article 15(3) and (4) of the MB Decision 58/2015 requires that Frontex make a provisional evaluation of the necessity of the transfer to Europol. To contribute to this evaluation, Europol must supply in advance in specific Operational Plans:

- the categories of data that are required from the operational area;
- the nationalities that are of current interest from the operational area;
- the areas of crime that are of current interest in the operational area; and
- the geographical locations (e.g. countries of origin, transit, departure) which are of current interest.

Paragraphs 5 and 6 of the same Article provide that personal data that match one or more criteria of the above list are considered as passing the evaluation of necessity and may be transferred to Europol.

However, the EDPS stresses that all the criteria of the above list are required (not only one or several of them as mentioned in Article 15 paragraphs 5 and 6 of MB Decision 58/2015) to comply with Frontex's legal obligation to assess the strict necessity of exchanging operational personal data with Europol, Eurojust and/or MS competent law enforcement authorities (Article 90 (2) of EBCG Regulation), i.e. whether the operational personal data that is exchanged strictly meet the recipients' prior requests.

Finding 21	Frontex does not carry out a necessity assessment before sharing the data packages with Europol. Frontex automatically shares each and every accepted interview report.
Finding 22	The feedback that Frontex receives from Europol is restricted [redacted]

Opening of an investigation

[168] Audit activities have revealed that a new working agreement negotiated with Europol and reflecting the latest legal framework is currently put on hold, see audit minutes p.35

Finding 21 indicates that Frontex has breached Article 71 (1) (c) of Regulation 2018/1725, Article 90 (2) (a) of the EBCG Regulation and Article 15(3) and (4) of the Frontex Management Board Decision 58/2015 by not assessing the strict necessity of sharing data packages with Europol, for the performance of its mandate. Such practice presents risks for the fundamental rights and freedoms of the data subjects. The impact on them is severe as the data minimisation principle is not complied with and data subjects that may not be of interest for the tasks of Europol would end up in their systems. The EDPS has thus decided to open an investigation.

Recommendations

Furthermore and without prejudice to the outcome of the investigation, the EDPS deems necessary that Frontex:

Recommendation 17	Determine the criteria on which the strict necessity assessment of the exchange of operational personal data by Frontex with Europol will be carried out. These criteria can include indicators that are necessary for Europol to perform its mandate.
Deadline	Three months following receipt of this report

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendation **within the specified deadline**.

4.1.4.5 Exercise of data subject rights

The audit activities have found that in case of a data subject access request in relation to the debriefing reports, Frontex cannot search the system with personal data (e.g. with the name of the data subject) but has to go through all interview reports.[169]

The right of access enables data subjects to check both whether their personal data are correct and whether they are being lawfully processed. It is a cornerstone of the right to data protection and is explicitly granted by Article 8 (2) of the European Charter of Fundamental Rights (the 'Charter'). Through the right of access, data subjects can also monitor whether central data protection principles such as data minimisation,

[169] Refer to audit minutes, p.29-30

purpose limitation and storage limitation are being complied with. The possibility to exercise this right is all the more important in cases under consideration where the personal data have been collected from another source than the individuals concerned who are therefore not aware that their data are processed by Frontex and further exchanged with Europol.

Finding 23	Frontex does not have tool(s) to search whether systems storing debriefing reports contain personal data about a specific individual in order to comply with a data subject access request.

Recommendation

In order to avoid risks of non-compliance with Article 17 and Article 80 of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 18	Implement appropriate ways to search debriefing reports and retrieve information regarding a data subject when handling a request for access.
Deadline	Six months following receipt of this report

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendation **within the specified deadline.**

4.1.4.6. Processing of data collected from debriefing interviews for purposes of risk analysis (Article 29)

A) Debriefing interviews as source of information for risk analysis

Debriefing interviews are used to gather information on modus operandi of apprehended irregular migrants, migration routes and related serious criminal activities such as migrant smuggling, traffic of human being, drug trafficking, documentary fraud, and terrorism.

This information is then used for purposes of risk analysis, in particular for the drafting of operational analysis reports and third countries analysis reports. They however constitute only one source of information for the

production of these reports. Frontex explained that the methodology for producing risk analysis has shifted from descriptive analyses based primarily on statistics to risk analyses based on the fusion of different data sources (in terms of quality and quantity). These sources include:

[redacted]

[redacted]

[redacted]

b) Legal basis (lawfulness)

Article 4(1)(a) of Regulation 2018/1725 requires personal data to be processed lawfully (principle of lawfulness), i.e. in accordance with the applicable legal framework. It is thus first necessary to establish whether Frontex has sufficient legal basis to process the personal data collected during debriefing interviews for purposes of risk analysis.

---

170 As explained by Frontex and verified by the EDPS audit team, Incident Reports are not designed to collect personal data: fields include information on 'person' (e.g. irregular migrant') 'age', 'presumed nationality', 'confirmed nationality', 'gender', 'outcome', 'documents' (with the possibility to attach documentation (e.g. copied of forged documents or technical equipment mission reports) to the report. Minutes, p.19

171 Minutes, p.6 and p.18

172 Minutes, p.19 « International Organisation for Migration (IOM) Missing Migrants Project (for weekly reporting) and open source data (e.g. from the UNHCR) as well as information provided by Liaison Officers in Member States (e.g. on policy changes, imposition of a state of emergency) as examples. He referred to the fact that other EU agencies may provide data, but they are primarily recipients of risk analyses (e.g. the Europol monthly report)."

173 Minutes, p.19-20

174 Minutes, p.19

According to Frontex[175], risk analysis is the starting point for all Frontex activities, from high level strategic decision-making to planning and implementation of operational activities.

Frontex collects a wide range of data from Member States, EU bodies, its partner countries and organisations, as well as from open sources on the situation at and beyond Europe's borders. The data is analysed with the aim of creating a picture of the situation at the EU's external borders and the key factors influencing and driving it.

Beyond establishing trends and identifying risks, Frontex also provides advice on appropriate operational responses to various challenges, including cross-border crime, at the EU external borders, including for daily coordination of Joint Operations. This helps to optimise the use of available resources and maximise the effectiveness of actions taken.

Frontex's risk analysis activities fall into three categories:[176]

- Strategic Analysis, aimed mostly at high-level strategic decision-makers. It indicates migratory trends and related indicators;[177]
- Operational Analysis, supporting Frontex-coordinated Joint Operations;
- Third Country Analysis, committed to long-term cooperation with external partners in regions where challenges for the EU external border originate and which they pass through (Western Balkans, Turkey, Eastern Partnership, and Africa).

Article 87(1)(e) of the EBCG Regulation authorises Frontex to process personal data for the purposes of risk analysis in accordance with Article 29 EBCG Regulation.

Article 29 of the EBCG Regulation tasks Frontex with the monitoring of migratory flows towards the Union, and within the Union in terms of migratory trends, volume and routes, and other trends or possible challenges at the external borders and with regard to return. For that purpose, Frontex shall establish a common integrated risk analysis model,

---

175 https://frontex.europa.eu/we-know/situational-awareness-and-monitoring/monitoring-risk-analysis/#:~:text=Frontex%27s%20risk%20analysis%20activities%20fall,supports%20Frontex%2Dcoordinated%20Joint%20Operations

176 For a list of the types of analytical reports generated and used by Frontex see Guidelines for Risk Analysis Units: Structures and Tools for the use of CIRAM, V.2.0, p.60.

177 Frontex, Risk analysis for 2021, p.6, https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Risk_Analysis_2021.pdf

which shall be applied by Frontex and the Member States. The Common Integrated Risk Analysis Model (CIRAM) was updated in June 2021.

Frontex explained that a risk is defined therein as a function of and consists of three pillars: threat, vulnerability and impact. It includes eight steps in the intelligence cycle: definition of scope of intelligence exercise tasking, data collection, evaluation of the information, selection, collation, analysis and interpretation, reporting, dissemination and review. It focuses on all four levels of the four-tier access control model for European Integrated Border Management (EIBM)[178] and shall cover all aspects relevant to EIBM with a view to developing a pre-warning mechanism, in line with Article 29(3) of the EBCG Regulation. While the EBCG Regulation does not define the concept of "pre-warning mechanisms", it can be understood as an early warning system, i.e. a system used to receive information or alert other stakeholders about expected or current risks or threats related to, e.g., movements of persons or goods.[179]

Article 29(2) of the EBCG Regulation also mandates Frontex to prepare tailored risk analyses for operational activities. These risk analyses shall cover all aspects relevant to EIBM with a view to developing a pre-warning mechanism, in line with Article 29(3) EBCG Regulation.

To that end, Article 29(5) of the EBCG Regulation creates an obligation for MS to provide Frontex with all necessary information regarding the situation, trends and possible threats at the external borders and in the field of return. MS shall regularly, or upon request of Frontex, provide it with all relevant information such as statistical and operational data collected in relation to European integrated border management that is included in the list of mandatory information and data to be exchanged with Frontex as defined in a Decision from the Management Board[180], as well as information from the analysis layers of the national situational pictures.

---

178 The EIBM is based on the four-tier access control model, which comprises measures in third countries, measures with neighbouring third countries, border control measures at the external borders, and measures within the Schengen area and return. Frontex and the Member States should take and adjust measures in all tiers based on risk analysis. (COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL establishing the multiannual strategic policy for European integrated border management, COM(2023) 146 final, Strasbourg, 14.3.2023.

179 See for example, European Commission, Guidelines for Integrated Border Management in European Commission External Cooperation, November 2010, https://www.icmpd.org/file/download/48280/file/Guidelines%2520for%2520Integrated%2520Border%2520Management%2520in%2520European%2520Commission%2520External%2520Cooperation%2520EN.pdf

180 Article 100(2)(e) EBCG Regulation

In turn, under Article 29(7), Member States shall take results of the risk analysis into account when planning their operations and activities at the external borders and their activities with regard to returns.

In light of the above, it can be established that Frontex has sufficient legal basis to process the personal data collected in the context of debriefing interviews for the purpose of risk analysis.

Finding 24	The information contained in the debriefing interviews are used for the production of the following risk analysis products: [redacted]
Finding 25	As long as debriefing interviews are used to gather information on modus operandi of apprehended irregular migrants, migration routes and related serious criminal activities such as migrant smuggling, traffic of human beings, drug trafficking, documentary fraud, terrorism, this information appears relevant to allow Frontex to fulfil its task under Article 29 and thus for the purpose of risk analysis.

C) ADEQUACY OF THE INFORMATION COLLECTED DURING DEBRIEFING INTERVIEWS (DATA MINIMISATION)

Article 4(1)(c) of Regulation 2018/1725 requires the processing of personal data to be limited to data that are adequate, relevant and necessary in relation to the purposes for which they are processed ('data minimisation').

The interviews have shown that the information collected during these debriefing interviews is of low reliability, partly because of the conditions of collection (see above section 4.1.4.3).

All nine debriefing interviews sampled by the Audit Team A were marked with the lowest level of reliability.[181] The DOs interviewed by Team B explained that in principle they cannot assess the quality (reliability) of the source and therefore they assign to it the lowest grading level (i.e. D). The same applies to the quality (accuracy) of the information, to which they also in principle assign the lowest grading level (i.e. 4). No specific criteria or guidance other than the one provided in the Handbook to the Operational Plan were mentioned by the DOs for evaluating the reliability

[181] Minutes, p.30

of the source and the validity of the information collected via debriefing interviews.[182]

However, the inspection activities revealed that, in four out of seven interview reports sampled by the EDPS audit team B, the accuracy of the information was assessed as belonging to a higher category (in two cases it was assessed as category 2[183], while in the other two as category 3[184]). Moreover, in one out of seven interview reports the reliability of the source was assessed as belonging to category C[185].

It is relevant in this context to refer to the decision of the Spanish Ombudsman, of 11 November 2022[186] stressing that the observed lack of minimum procedural safeguards during these debriefing interviews, such as deficiencies in communication with the interviewee, the time of the interview and its lack of confidentiality, can have an impact on the quality of the information gathered.

Finding 26	The information collected during these debriefing interviews is of low reliability.

Given the low reliability of the information collected in the context of debriefing interviews, the EDPS tried to get an understanding of the practical importance and usefulness of the information collected in the context of debriefing interviews for purposes of risk analysis in order to assess whether these data are adequate, relevant and necessary in relation to the purposes for which they are processed.

Here, the EDPS did not get a clear understanding of the amount of the debriefing interview reports used nor methodology applied to build risk analysis related documents (such as bi-weekly reports), namely whether, and to what extent, the information from the debriefing interview is treated as an important and credible source of information for Frontex. The interviews conducted by the EDPS[187], and the risk analysis products identified, show that there might be a certain potential usefulness of

[182] Minutes, p.10

[183] Information known personally to the source but not know personally to the official passing it, Handbook on OPLAN, June 2022, p. 114

[184] Information not known personally to the source but corroborated by other information already recorded, Handbook on OPLAN, June 2022, p. 114

[185] The source from whom/where the information was received has in most instances proved to be unreliable.

[186] Defensor del Pueblo, Decision on Frontex Operational Plans in Spain, §9, https://www.defensordelpueblo.es/resoluciones/planes-operativos-de-las-actuaciones-de-frontex-en-espana/

[187] Minutes, p.17-22

information collected at debriefing interviews, although of rather ancillary nature, not impacting most significantly Frontex's ability to deliver the operational risk analysis products (as they are mostly based on other sources, [redacted]). It is thus not clear whether the processing of data collected in the context of debriefing interviews are necessary for the purpose of risk analysis, within the meaning of Article 4(1)(c) of Regulation 1725/2018.

In addition, and exacerbating the difficulties encountered by the audit team to properly assess the relative weight placed on debriefing reports for risk analysis, the audit team noted[188] that there is no clear mapping of the processing of personal data and other information conducted by Frontex for Risk Analysis purposes, which identifies in a comprehensive manner the sources of information feeding risk analysis (as well as the forms of analysis performed on the data and information gathered). It was therefore not possible for the audit team to document exhaustively the categories and flows of personal data which feed into Frontex's risk analysis products. This is not only problematic from an auditing and self-monitoring perspective, but may also lead to limitations when attempting to verify the evidence base upon which risk analyses and resulting operational instructions rely (risk of a black box).

The EDPS audit team was also not able to obtain a clear understanding of how the low level of reliability of the information collected in the context of debriefing interviews was compensated or even taken into account in the methodology for producing risk analysis.

The EDPS is concerned by the fact that the use of information of low reliability for the production of risk analyses might have a negative impact on certain segments of people on the move, who would end up being unduly targeted by more stringent security measures or increased border checks, thus impinging in their right to non-discrimination. This might also have a chilling effect on their travel behaviour and thus on their ability to move freely. In these cases, risk analyses do not only affect individuals, who may have acted differently from the rest of the group to which they have been assigned, but also affects the whole group and sets it apart from the rest of society. The EDPS is concerned that the strategies used to group data and the logic of data analytics and the potential bias induced by the use of unreliable information have an influence on the final representation of groups and society.[189] These risks will only aggravate as

[188] Minutes, p.17-22

[189] See in that sense, Mantelero A., Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review 32 (2016) 238-255.

the information available increases and Frontex starts using software analytics to process these data.

In light of the aforementioned risks to individuals, the EDPS has doubts as to whether the processing of personal data collected in the context of debriefing interviews are adequate and relevant, within the meaning of Article 4(1)(c) of Regulation 1725/2018.

The EDPS further recalls that under Article 80 EBCG Regulation, Frontex has the duty to guarantee the protection of fundamental rights in the performance of its tasks under the Regulation in accordance with relevant Union and international law. In its Fundamental Rights Strategy adopted on the basis of this Article, Frontex commits to ensure that the methodology applied for risk analysis considers and reflects the impact on the rights of persons crossing the borders.[190]

To this end, the EDPS believes that the use of debriefing interviews for the risk analysis purposes by Frontex should be carefully assessed. This purpose (i.e. risk analysis) is nonetheless one of the two reasons why Frontex does conduct debriefing interviews. These not only result in a collection of personal data from an individual, but occur in a sensitive and vulnerable environment (on which the EDPS has identified specific findings and recommendations in this report). Such data collection requires the ability of Frontex, in its role as controller, to explain precisely the purposes and relevance of such data collection, in line with the principles of data minimisation (Articles 4(1) and (c) of Regulation 2018/1725).

Finding 27	There is no comprehensive overview of the processing of data and information conducted by Frontex for Risk Analysis, detailing in an exhaustive manner the sources of information feeding risk analysis (as well as the forms of analysis performed on the data and information gathered).
Finding 28	The EDPS is concerned that the low reliability of the information collected in the context of debriefing interviews is not sufficiently taken into account in the methodology used by Frontex to produce risk analysis to ensure that they do not have an influence on the final representation of groups in particular as risk

[190] Fundamental Rights Strategy, endorsed by the Fundamental Rights Officer on 25 January 2021 and adopted by the Management Board on 14 February 2021, Warsaw, p.6

	analysis products ultimately inform the policy decision-making process

Recommendations

In order to avoid risks of non-compliance with Article 4(1)(b) and (c) of Regulation 2018/1725, and to avoid the risk of discrimination of certain group of people on the move due to the inaccuracy of the information collected during the debriefing interviews, in accordance with Article 80 of the EBCG Regulation, the EDPS deems necessary that Frontex:

Recommendation 19	Perform a risk assessment and, where relevant, adopt mitigation measures to ensure that the unreliable nature of information collected in the context of debriefing interviews and further used for the risk analysis process does not affect the reliability of the conclusions of the risk analyses.
Deadline	Three months following receipt of this report
Recommendation 20	Undertake a mapping of processes that fall within the scope of risk analysis, including a comprehensive identification of information and data sources, and analytical tools applied that would include the following minimum elements: • list of all risk analysis products, • list of all risk analysis products that use the information from the debriefing interviews • list of other sources of information used in these products, • number of debriefing interviews reports used in preparation of these products • comparison of the usefulness of all sources of information used in these products (for each product separately).
Deadline	Three months following receipt of this report

The EDPS expects that Frontex provides documentary evidence of the implementation of the above recommendations **within the specified deadlines.**

4.2. Data protection by design and by default

During the interviews, Frontex presented the technical architecture that supports the screenings/debriefings to the audit team.[191] The following sections describe elements concerning data protection by design and by default, as described in Article 27 of Regulation 2018/1725, that were discussed during the audit, which the EDPS considers relevant to address.

4.2.1 Background

Data protection by design and by default (DPbDD) is a legal requirement laid down in Articles 27 and 85 of Regulation 2018/1725 for any processing of personal data. This requirement has been further interpreted by the European data Protection Board in its EDPB guidelines on DPbDD.[192] According to the EDPB, each step of each process must be examined in the light of the principles of transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability to determine how best to integrate data protection. This in turn leads to an analysis of the risks to the data subjects and the specification of technical and organisational measures typically.

DPIA on systems

A DPIA is a tool to evaluate the risks to data subjects and come up with corresponding safeguards to minimise those risks. DPIAs are usually carried out by analysing a processing operation. When the processing operation changes (for example when additional functionalities are required), then the corresponding DPIA must be reviewed.

Consultation of the DPO on internal decisions affecting the processing of personal data

[191] The meetings are described in the audit minutes. Sections “TEAM C: Description of the technical architecture that supports the screenings/debriefings/intelligence reports including the IT systems involved in the processing of personal data (including PeDRA, JORA and non-JORA)” (pages 16-17), “TEAM C: - Live demonstration of the PeDRA and JORA systems and Demonstration and interviews with the staff involved in anonymisation and data retention of personal data used for risk analysis” (pages 26-29) and “TEAM C: Description of the software development, deployment and maintenance strategy, product management and change management procedure for the systems involved in the screening/ debriefing/intelligence reports activities and Demonstration of the measures of data protection by default and by design that are implemented on the screening/debriefing/reporting activities” (pages 38-41).

[192] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0, adopted on 20 October 2020).

Operations on personal data are typically assessed in order to minimise the risks to data subjects. This is why it is important to have data protection experts performing these assessments. The DPO is a key resource in any organisation to help either in the analyses themselves or as an additional safeguard to ensure that the analyses are performed and performed adequately. In any case, to have an effect, the DPO should be informed and/or consulted to enable her/him to make use of her/his expertise.

Testing with operational data

Testing a system is an important part of the development lifecycle that needs to take place before putting a system in production.

Testing should be done at different levels:

- By developers, to ensure that the products behave as expected;
- By IT operational staff, to ensure that the programming can be integrated into the IT environment;
- By a mix of users and consultants, to ensure that the software meets the specifications (the documents drafted on which the programming is based); and
- By users, to ensure that the software fulfils their needs.

Usually, it is not recommended to use operational data to build these datasets for testing purposes as it creates additional information security risks and, more importantly, from a data protection perspective, needs to be duly justified inter alia in terms of lawfulness, necessity, proportionality and data minimisation, and be supported by a policy document and a procedure.

Mechanism for DPO to monitor logs

A key safeguard in the realm of DPbDD is to enable a DPO to perform internal auditing of the use of operational personal data for compliance monitoring purposes. Her/his checks allow detecting misuse of personal data and even data breaches. To that end, a DPO requires tools to make sense of the application logs (logs of the use of personal data) as well as access to these logs.

4.2.2 Criteria

The following provisions of **Regulation 2018/1725** are of particular relevance in this context

- Articles 27 and 85 on data protection by design and by default

- Articles 39 (1) and 89 (1) on the obligation for the controller to carry out a DPIA.
- Article 39 (2) on the obligation for the controller to seek the advice of the DPO when carrying out a DPIA.
- Article 44 (1) on the obligation to involve the DPO properly and in a timely manner, in all issues which relate to data protection.
- Article 45 (1) (b) on the tasks of the DPO.
- Article 88 on logging.

The following standard is also of relevance for the legal assessment:
- ISO 27002:2022 (8.33 - test information and 5.34 - privacy and protection of PII).

4.2.3 Actions

During the on-site activities, the audit team (team C) carried out interviews aiming at:
- securing a common high level overview of the three main data processing activities that will be further audited by teams A (processing of data for risks analysis purposes), B (processing of data for law enforcement purposes) and C (processing of data in JORA system) and,
- understanding the involvement of different Frontex' divisions/units in the data flows regarding screening/debriefing and intelligence reports activities.

The information obtained during these common interviews was completed with additional interviews and checks on Frontex's IT systems to understand how the information contained in the debriefing reports are processed on the IT systems.

The EDPS interviewed Frontex team members responsible for conducting the debriefing interviews of the migrants, Frontex's staff members responsible for the use of information collected at the debriefing interviews either for further transmission of operational data to Europol (PeDRA) or for risk analysis (in various forms) and Frontex IT Technical staff members.

The Data Protection Office(r) attended the interviews, which were followed by hands-on checks.

All audit activities are described in detail in the audit minutes. The next section will focus on the most relevant audit activities and in particular on activities which triggered findings and recommendations.

4.2.4 Findings and recommendations

a) Lack of timely DPIA on systems

JORA2 is a system in which modules can be added over time, depending on the changing business needs. Currently, Frontex is developing two new modules that process personal data: the debriefing interview module and the intelligence report module. Frontex reported that the DPIA on JORA2 for these modules is still ongoing[193].

According to Frontex, the DPIA will be done module by module until it covers the whole JORA2 system. The contracts that were drawn up when the software was to be developed contained data protection clauses which were integrated, but have no DPIA to support them[194].

Opera EVO, a customized application to support operational activities, also has a DPIA in progress but not yet completed. This system processes personal data of a large number of Frontex employees, including history of deployment, job profile and identity photography for the purpose of managing resources during mission.

According to Articles 39 and 89 of Regulation 2018/1725, a DPIA should be carried out for processing operations using new technologies, while taking into account the nature, scope, context and purposes of the processing, and its likeliness to result in a high risk to the rights and freedoms of natural persons. According to Articles 39 (1) and 89 (1) of Regulation 2018/1725, the DPIA should take place prior to the data processing.

The conclusions of this assessment on the protection of personal data should then be implemented on the existing system. The DPIA should lead to a set of controls to mitigate the risks. These controls should then be implemented as part of the system's development.[195]

[193] See minutes p19-20

[194] During the audit, Frontex reported that no DPIA was received from the contractor and that Frontex did not participate in a contractor's DPIA either.

[redacted]

The DPIAs will help identifying appropriate technical and organisational measures that should be implemented on the existing production environments (after due care is take to test the new controls and deploy them according to sound change management processes.

It should be noted that **all** systems/modules processing personal data should have a DPIA.

Moreover, Article 39 (11) of Regulation 2018/1725 defines that, *where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations*.

Should the DPIA highlight an unavoidable high risk to data protection for a system already in production, the controller would need to re-design the system and in worst case scenarios would need to stop operations (i.e. shut down the system).

Finding 29	Frontex did not prepare DPIAs as required (before the start of any processing operation. DPIAs. DPIAs should be carried for systems/modules processing personal data likely to result in a high risk to the rights and freedoms of natural persons. This analysis will help identifying controls that should be implemented on new and existing systems.

Recommendation

In order to avoid risks of non-compliance with Article 86(1) of EBCG Regulation and Articles 39 and 45(1)(b) of Regulation 2018/1725, the EDPS recommends that Frontex:

Recommendation 21	Identify the processing operations which could result in a high risk to the rights and freedoms of natural persons (in line with Article 39

[195] However, it should be taken into account that the DPIA results are not the only thing to do to be aligned with DPbDD.

	Regulation 2018/1725) and perform the corresponding DPIAs. Subsequently, controls should be implement to address the identified risks.

In light of the accountability principle laid down in Article 4 (2) of Regulation 2018/1725, the EDPS expects Frontex to implement the above recommendation accordingly.

B) ABSENCE, OR DELAY, IN CONSULTING THE DPO ON INTERNAL DECISIONS AFFECTING THE PROCESSING OF PERSONAL DATA

In terms of software changes, a team composed of subject matter experts (from areas of ICT, business and security) deals with the changes and evaluate if these changes affect data protection. In those cases, the DPO is consulted. The prioritisation of changes is discussed with the operational team responsible for the interviews at the border but the final decision goes to the product owner. There is no specific data protection expert profile in the team.
Additionally, the DPO was not involved in the drafting of the platform requirements. The DPO will be consulted once there is a specific solution envisaged.

While the identification of the presence of operations involving processing of personal data is, ultimately, a task up to the data controller, it is also true that the data controller can seek the advice of the DPO (Regulation 2018/1725 (Article 45)).

The EDPS considers that involving the DPO in the requirement gathering and choice of information systems is a good practice[196], which facilitates compliance of the data controller with Regulation 2018/1725 and further involves the DPO in the details of the organisation systems.

The Frontex DPO is not sufficiently involved at the early stages of the design, or the market search, of software solutions that may involve the processing of personal data[197]. There is no sufficient guarantee that the product owners have the necessary know-how to correctly identify the possible impacts of data processing on individuals, nor that they are able to identify data protection requirements for new products, or changes to existing products.

[196] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

[197] See minutes p21

Hence, there is a risk that DPbDD principles are not sufficiently taken into account for Frontex systems, as defined in Articles 27 and 85 of Regulation 2018/1725.

Finding 30	The DPO should be allowed to fulfil her role fully by being involved in all process that include the processing of personal data.

Recommendation

In order to avoid risks of non-compliance with Article 86(1) of EBCG Regulation / and Articles 39 and 45(1)(b) of Regulation 2018/1725, the EDPS recommends that Frontex:

Recommendation 22	Review all processes in which processing of operational data is present and involve the DPO in order to provide an input with regards to these processing operations.

In light of the accountability principle laid down in Article 4 (2) of Regulation 2018/1725, the EDPS expects Frontex to implement the above recommendation accordingly.

c) Lack of procedure defined for testing with operational data

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

Finding 31	[redacted]

Recommendation

In order to avoid risks of non-compliance with Article 86(1) of the EBCG Regulation / and Articles 39 and 45(1)(b) of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 23	[redacted].
Deadline	Six months following receipt of this report

The EDPS expects Frontex to provide documentary evidence of the implementation of this recommendation (i.e. techniques and methodology used to create or acquire the test data) **within the specified deadline**.

D) Lack of mechanism for DPO to monitor logs

Article 88 Regulation 2018/17205 requires the controller to keep logs for processing operations in automated processing systems for the verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the operational personal data and for criminal

[199] See minutes p 47

proceedings. Under Article 45 (1) (b) Regulation 2018/1725, the DPO must "ensure in an independent manner the internal application of this Regulation; monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits".

This requires that:

- The application logs contain the complete and relevant information that would allow the DPO to fulfil her tasks; and
- Tools are created to fulfil the needs of the DPO in terms of auditing operational personal data

Frontex did not foresee before the development that the DPO should also be considered as a user of the production system with specific needs in terms of data protection[200]. One such need is the ability to audit the use of operational personal data. This requires that the application logs contain sufficient data and have a tool to search the logs in a meaningful way.

The DPO should be the one determining what data and functionalities are necessary to fulfil its task of monitoring compliance with the Regulation 2018/1725 in an independent manner (as foreseen in Article 45 (1) (b) of Regulation 2018/1725).

Finding 32	There is no tool to read application logs in a meaningful manner for the DPO [redacted]

Recommendation

In order to avoid risks of non-compliance with Article 86(1) of EBCG Regulation and Articles 39 and 45(1)(b) of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 24	Identify what are the needs in terms of auditing the operational systems containing personal data for the DPO and for the staff responsible for managing the system [redacted]

[200] See minutes p47

	Subsequently, the necessary information should be recorded in the application logs and a tool should be built according to the DPO's specifications to ensure that she can use the application logs to fulfil her obligations (according to Article 45 (1) b) Regulation 2018/1725).
Deadline	Six months following receipt of this report

The EDPS expects Frontex to provide documentary evidence of the implementation of this recommendation **within the specified deadline**.

4.3 Security of the information systems

During the interviews, Frontex presented the technical architecture that supports the screenings/debriefings to the audit team.[201] The following sections describe elements of the information security management of Frontex that were discussed during the audit, which the EDPS considers relevant to address.

4.3.1 Background

[redacted]

[201] The meetings are described in the audit minutes. Sections "TEAM C: Description of the technical architecture that supports the screenings/debriefings/intelligence reports including the IT systems involved in the processing of personal data (including PeDRA, JORA and non-JORA)" (pages 16-17), "TEAM C: - Live demonstration of the PeDRA and JORA systems and Demonstration and interviews with the staff involved in anonymisation and data retention of personal data used for risk analysis" (pages 26-29) and "TEAM C: Description of the software development, deployment and maintenance strategy, product management and change management procedure for the systems involved in the screening/ debriefing/intelligence reports activities and Demonstration of the measures of data protection by default and by design that are implemented on the screening/debriefing/reporting activities" (pages 38-41).

[202] Minutes, p.26

[203] Debriefing interviews are described in pages 5 to 8 of the audit minutes

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[204] Using short messages (SMS) or PUSH notifications to send challenges or one-time passwords.

[205] Minutes, p.41

[206] Minutes, p.16

[207] JEVO Technical Design Document.

[208] Discontinued software is no longer developed or maintained by the original developer.

[209] Minutes, p.28-29

[redacted]

[redacted]

[redacted]

4.3.2 Criteria

The following provisions of **Regulation 2018/1725** are of particular relevance in this context:

- Article 15(2) on the need to manage information security in order to operate an information system capable of exchanging classified and sensitive non-classified information, and of exchanging personal data.
- Article 33 (1) on the obligation for the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

One such organisational measure contributing to data protection is adhering to internationally and industry recognised IT standards and best practices in the governance and management of information systems. In this context, the EDPS took into consideration the international standard **ISO/IEC 27002:2022** (Information security, cybersecurity and privacy protection — Information security controls).

In particular, the following controls:

- Control 5.14 (Information transfer), which defines that, for all types of information transfer, rules, procedures and agreements should include a) *controls designed to protect transferred information from interception, unauthorized access, copying, modification, misrouting, destruction and denial of service, including levels of access control commensurate with the classification of the information involved and any special controls that are required to protect sensitive information, such as use of cryptographic techniques*;

[210] Minutes, p.17

- Control 5.18 (Access rights), which states that *access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control*;
- Control 8.5 (Secure Authentication), which states that *the strength of authentication should be appropriate for the classification of the information to be accessed. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as digital certificates, smart cards, tokens or biometric means, should be used*;
- Control 8.8 (Management of technical vulnerabilities), addresses the importance of identifying systems with potential vulnerabilities, evaluating the risks and applying appropriate measures;
- Control 8.16 (Monitoring activities), addresses the fact that *continuous monitoring via a monitoring tool should be used. Monitoring should be done in real time or in periodic intervals, subject to organizational need and capabilities. Monitoring tools should include the ability to handle large amounts of data, adapt to a constantly changing threat landscape, and allow for real-time notification. The tools should also be able to recognize specific signatures and data or network or application behaviour patterns.*

4.3.3 Actions

During the on-site activities, the audit team (team C) carried out interviews aiming at:

- securing a common high level overview of the three main data processing activities that will be further audited by teams A (processing of data for risks analysis purposes), B (processing of data for law enforcement purposes) and C (processing of data in JORA system) and,
- understanding the involvement of different Frontex' divisions/units in the data flows regarding screening/debriefing and intelligence reports activities.

The information obtained during these common interviews was completed through additional interviews and demonstrations on Frontex's IT systems to understand how the information contained in the debriefing reports are processed on the IT systems.

The EDPS interviewed Frontex team members responsible for conducting the debriefing interviews of the migrants, Frontex's staff members responsible for the use of information collected at the debriefing interviews either for further transmission of operational data to Europol (PeDRA) or for risk analysis (in various forms) and Frontex IT Technical staff members.

The Data Protection Office attended the interviews, which were followed by hands-on demonstrations.

All audit activities are described in detail in the audit minutes. The next section will focus on the most relevant audit activities and in particular on activities which triggered findings and recommendations.

4.3.4 Findings and recommendations

a) Concerning the risks associated with control objective ISO 27002:2022 8.5 – Secure Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Services authenticated from the internet have a greater exposure to attacks given that anyone can access the site hosting the services on a public network (i.e. the Internet). In these circumstances, any potential bad actor can access to the internet-facing login page and try to access the reserved area with stolen credentials. [redacted]

[redacted]

Control 8.5 is a preventive control that mitigates risk through the implementation of technology and topic-specific secure authenticate processes that ensure that human and nonhuman users and identities

undergo a robust and secure authentication process whenever they attempt to access ICT resources.

According to Control 8.5 of ISO/IEC 27002:2022, a *suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities. The strength of authentication should be appropriate for the classification of the information to be accessed.*

The EDPS considers that, in order to implement an appropriate authentication technique, Frontex first needs to assess the possible security risks associated with the authentication mechanisms currently used for its web-based services providing access to systems processing personal data.

[redacted]

Finding 33	[redacted]

Recommendations

In order to ensure compliance with Article 33 (1) of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 25	[redacted]
Deadline	Three months following receipt of this report

The EDPS expects Frontex to provide documentary evidence of the implementation of the above recommendation (i.e. management approved security risk assessment) **within the specified deadline**.

Furthermore, the EDPS recommends that Frontex:

Recommendation 26	[redacted]

In light of the accountability principle, the EDPS expects that Frontex implements the above recommendation accordingly.

B) Concerning the risks associated with control objective ISO 27002:2022 8.8 – Management of Technical Vulnerabilities

JORA1 contains a repository of serious incident reports which may include personal data.[211]

Keeping discontinued systems running can pose serious security risks to organisations for the several reasons:

- Organisations often cease to provide updates and security patches to discontinued systems and their dependencies (e.g. application programming interface (APIs)). This means that these systems become outdated and might become vulnerable to attacks exploring unpatched flaws. Outdated systems can be exploited by attackers, or malware, to progress to other, more sensitive, systems (a practice known as *lateral movement*);
- Outdated systems might also require the use of other outdated software for compatibility purposes (for instance, older operating systems), which in turn results in more vulnerabilities to attacks;

[redacted]

According to Control 8.8 of ISO/IEC 27002:2022, the organization should identify technical vulnerabilities and, *once a potential technical vulnerability has been identified, identify the associated risks and the actions to be taken*.

No evidence of the existence of such a risk assessment has been provided by Frontex.

211 See section 4.1.4.1, subsection a) Incident Reporting

Finding 34	[redacted]

Recommendations

In order to avoid risks of non-compliance with Article 33 (1) of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 27	Conducts a security risk assessment that addresses the security risks [redacted]
Deadline	Three months following receipt of this report

The EDPS expects Frontex to provide documentary evidence of the implementation of thre above recommendation (i.e. management approved security risk assessment) **within the specified deadline**.

Furthermore, the EDPS recommends that Frontex;

Recommendation 28	Implement security mechanisms to adequately address the risks of [redacted] The residual risk resulting from the application of the mitigation measures to the risks identified as a consequence of Recommendation 27 should be approved by Frontex management

In light of the accountability principle laid down in Article 4 (2) of Regulation 2018/1725, the EDPS expects that Frontex implements the above recommendations accordingly.

c) Concerning the risks associated with control objective ISO 27002:2022 5.14 -Information Transfer

Email is a notoriously unsecure means of information exchange. First, because it circulates on a public network (i.e. the Internet), which is accessible by the public at large. Second, because, without additional controls, it is unencrypted in its basic form. Since an e-mail goes through different servers on its way to its destination (i.e. mail relays), anyone on the path can intercept the email and read, modify or even delete it.

In its simplest form, electronic mail (commonly known as e-mail) has no security controls to ensure the integrity nor the confidentiality of the message[212]. It should be considered unsuitable for the exchange of sensitive information unless additional security mechanisms are added (e.g. digital certificates for encryption and/or digital signature of the message).

According to Control 5.14 of ISO/IEC 27002:2022, procedures and agreements should include controls designed to protect transferred information from interception, unauthorized access, copying, modification, misrouting, destruction and denial of service.

The mechanism used for information exchange between Frontex and the MS (unencrypted email) might involve risks to the confidentiality and integrity of the information that Frontex needs to assess to be able to apply the adequate controls

No evidence of the existence of such a risk assessment has been provided by Frontex.

Finding 35	[redacted]

Recommendations

[212] Email messages are generally not encrypted and have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.

In order to avoid risks of non-compliance with Article 33 (1) b) of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 29	Conducts a security risk assessment addressing the security risks posed by the transfer of information outside the system and, [redacted]
Deadline	Three months following receipt of this report.

The EDPS expects Frontex to provide documentary evidence of the implementation of this recommendation **within the specified deadline.**

Furthermore, the EDPS recommends that Frontex;

Recommendation 30	[redacted] The risk assessment, the mitigation measure and the resulting residual risk should be approved by Frontex management

In light of the accountability principle laid down in Article 4 (2) of Regulation 2018/1725, the EDPS expects that Frontex implements the above recommendations accordingly.

D) CONCERNING THE RISKS ASSOCIATED WITH CONTROL OBJECTIVE CONTROL 8.16 – MONITORING ACTIVITIES

[redacted]

The importance of the systematic monitoring of logs is encompassed in Article 33 (1) d) Regulation 2018/1725, which addresses the need for controller and the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including *a process for regularly testing, assessing and evaluating the*

[213] Minutes, p.17

effectiveness of technical and organisational measures for ensuring the security of the processing.

Control 8.16 of ISO/IEC 27002:2022 also addresses the importance of having continuous monitoring via a monitoring tool providing real-time notification.

Finding 36	[redacted]

Recommendations

In order to avoid risks of non-compliance with Article 33 (1) b) of Regulation 2018/1725, the EDPS deems necessary that Frontex:

Recommendation 31	[redacted]
Deadline	Three months following receipt of this report.

The EDPS expects Frontex to provide documentary evidence of the implementation of this recommendation **within the specified deadline.**

Furthermore, the EDPS recommends that Frontex;

Recommendation 32	[redacted] The resulting residual risk to apply these measures to the risks identified in Recommendation 31 should be approved by Frontex management

In light of the accountability principle laid down in Article 4 (2) of Regulation 2018/1725, the EDPS expects that Frontex implements the above recommendations accordingly.

5. COMPILED LIST OF RECOMMENDATIONS AND DEADLINE FOR IMPLEMENTATION

The EDPS recommends that Frontex:

Recommendation 1	Formalise checks on the absence of personal data during Frontex Situation Centre verification of JORA incident reports and include this procedural step in the guidance issued by the Risk Analysis Unit.	In light of the accountability principle
Recommendation 2	Conducts a thorough reassessment of its procedures for processing debriefing reports and implements the necessary measures to ensure compliance with the full set of data protection requirements provided by Regulation 2018/1725 and by the EBCG Regulation.	Six months following receipt of this report
Recommendation 3	Establish, with respect to the phase of the data processing which consists in the collection of personal data via the debriefing interviews, a clear set of rules prohibiting the sharing of information originating from different stages of migrant reception and processing (registration, screening and debriefing). Such rules could be included, for instance, in the Joint Controllership Arrangement to be established with Member States (see recommendation 4).	Six months following receipt of this report
Recommendation 4	Complement the joint controllers' arrangement in line with Article 86 Regulation 2018/1725	Six months following receipt of this report
Recommendation 5	Conclude an arrangement in line with Article 28 Regulation 2018/1725 with the host Member State's competent authorities regarding the processing of personal	Six months following receipt of this report

	data of migrants.	
Recommendation 6	Make the essence of the joint controllers' arrangements available to the data subjects as required by Articles 28 (2) and 86 (2) of Regulation 2018/1725.	Six months following receipt of this report
Recommendation 7	Ensure that Fundamental Right Officer Monitors can attend the debriefing interviews. This recommendation should be understood as extending to other type of activities conducted by Frontex at the EU borders, such as screening interviews or patrolling activities, where collection of personal data might take place and where the possibility for the Fundamental Right Officer Monitors to attend is not ensured.	Immediately
Recommendation 8	Put in place additional safeguards to ensure that interviews are only conducted with persons in adequate mental and physical condition. This may include laying down a minimum time period for intercepted persons to be adequately assessed and received before undergoing interview.	Two months following receipt of this report
Recommendation 9	Take appropriate measures to ensure that in the context of debriefing interviews an access to legal assistance is provided should the person request it, i.e. in order to seek clarification as to the nature of the interview and potential consequences of their statement. Clear information about the nature, purpose and implications of the interview should be provided in a language of the interviewee's understanding, both verbally and in writing.	Four months following receipt of this report
Recommendation 10	Specify, applicable rules and legislation in a dedicated annex to	Six months following

	the Operational Plan/Specific Activity Plan in order to ensure compliance with national procedural requirements when interviewing persons deprived of their liberty/freedom of movement, and with legal guarantees under national criminal procedures.	receipt of this report
Recommendation 11	Ensure that Frontex officers do not take part in debriefing interviews if the support from an interpreter or cultural mediator is not of a professional nature.	One month following receipt of this report
Recommendation 12	Make sure that the use of personal belongings in debriefing interviews only takes place (i) when the voluntary nature of the use is strictly ensured and (ii) in compliance with applicable national laws. Applicable rules and legislation should be added to the above-mentioned annex to the Operational Plan/Specific Activity Plan.	Six months following receipt of this report
Recommendation 13	- Define, for each joint operation, the criteria used to meet the threshold of "reasonable grounds" to qualify a person as suspect of a cross-border crime, in line with the applicable national law. and, - Put in place safeguards to ensure that before transmitting operational personal data to Frontex, the [redacted] of the host Member State verifies and validates that personal data contained in the debriefing report only refer to persons for whom there are reasonable grounds to suspect they are involved in cross-border crimes, in line with the applicable national law.	Six months following receipt of this report
Recommendatio	Ensure that the specific cross-border	

n 14	crimes and the intelligence gaps, for which the collection of operational personal data by Frontex through debriefing activities is asked to support MS competent authorities in their fight against cross-border crime and Europol in the performance of its mandate, are clearly identified.	Six months following receipt of this report
Recommendation 15	Ensure that Frontex receives specific and targeted requests from Europol prior to the collection of operational personal data and their further transmission to Europol.	By end of 2023
Recommendation 16	Document the instructions transmitted by Frontex's [redacted] to the Debriefing officers	In light of the accountability principle
Recommendation 17	Determine the criteria on which the strict necessity assessment of the exchange of operational personal data by Frontex with Europol will be carried out. These criteria can include indicators that are necessary for Europol to perform its mandate.	Three months following the receipt of the report
Recommendation 18	Implement appropriate ways to search debriefing reports and retrieve information regarding a data subject when handling a request for access.	Six months following receipt of this report
Recommendation 19	Provide a risk assessment and mitigation measures to ensure that the unreliable nature of information collected in the context of debriefing interviews and further used for the risk analysis process does not affect the reliability of the conclusions of the risk analyses.	Three months following receipt of this report
Recommendation 20	Undertake a mapping of processes that fall within the scope of risk analysis, including a comprehensive identification of information and data sources, and analytical tools	Three months following receipt of this report

	applied that would include the following minimum elements: • list of all risk analysis products, • list of all risk analysis products that use the information from the debriefing interviews • list of other sources of information used in these products, • number of debriefing interviews reports used in preparation of these products • comparison of the usefulness of all sources of information used in these products (for each product separately).	
Recommendation 21	Identify the processing operations which could result in a high risk to the rights and freedoms of natural persons (in line with Article 39 Regulation 2018/1725) and perform the corresponding DPIAs. Subsequently, controls should be implement to address the identified risks.	In light of the accountability principle
Recommendation 22	Review all processes in which processing of operational data is present and involve the DPO in order to provide an input with regards to these processing operations.	In light of the accountability principle
Recommendation 23	[redacted]	Six months following receipt of this report
Recommendation 24	Identify what are the needs in terms of auditing the operational systems containing personal data for the DPO and for the staff responsible for managing the system [redacted]	Six months following receipt of this report

	[redacted] Subsequently, the necessary information should be recorded in the application logs and a tool should be built according to the DPO's specifications to ensure that she can use the application logs to fulfil her obligations (according to Article 45 (1) b) Regulation 2018/1725).	
Recommendation 25	[redacted]	Three months following receipt of this report
Recommendation 26	[redacted]	In light of the accountability principle
Recommendation 27	Conduct a security risk assessment that addresses the security risks [redacted]	Three months following receipt of this report
Recommendation 28	Implement security mechanisms to adequately address the risks [redacted] The residual risk resulting from the application of the mitigation measures to the risks identified as a consequence of Recommendation 27 should be approved by Frontex management	In light of the accountability principle
Recommendation 29	Conduct a security risk assessment addressing the security risks posed by the transfer of information outside the system and, [redacted]	Three months following receipt of this report

	[redacted]	
Recommendation 30	[redacted] measure and the resulting residual risk should be approved by Frontex management	In light of the accountability principle
Recommendation 31	[redacted].	Three months following receipt of this report
Recommendation 32	[redacted] The resulting residual risk to apply these measures to the risks identified in Recommendation 31 should be approved by Frontex management.	In light of the accountability principle

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

6.ANNEXES

Annex 1 Powers of the EDPS

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

(1) 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) 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) 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 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 EDPS pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedies and due process, set out in Union law.

Annex 2 Documents collected prior to the audit

NO	DOCUMENT NAME
1.	DPO Annual Activity and Compliance Report 2021, Warsaw 24 February 2022, Ref: DPO/MANO/1443/2022
2.	Organisational structure of the European Border and Coast Guard Agency as established by the Management Board Decision No 18/2017 and further detailed by Decision of the Executive Director (FRONTEX INTERNAL STRUCTURE and Heads of entities)
3.	Frontex organisational structure
4.	DPIA Methodology
5.	The RAU data controller, Warsaw 2 May 2016
6.	PeDRA intake process - Process description
7.	Standard Operating Procedure - Reporting and pre-processing of information and operational personal data in the JORA interview report
8.	Handbook to the Operational Plan- Version June 2022 - Frontex Operational Activities, Warsaw 01/06/2022
9.	Presentation PowerPoint on PeDRA - Interview Reporting Module Workshop for TLs and IOs
10.	Presentation PowerPoint on PeDRA - Interview Reporting Module Workshop
11.	Presentation PowerPoint on Personal Data - PeDRA workshop
12.	Operational analysis sector organigram
13.	NORMALIZING PERSONAL DATA, Warsaw 25 May 2016
14.	ListOfVidTutorialsForDEBs
15.	ListOfVidTutorialsForTL&IO
16.	Common Integrated Risk Analysis (CIRAM), Version 2.1
17.	Guidelines for Risk Analysis Units - Structure and tools for the application of CIRAM version 2.0
18.	PRODUCT CARD: Annual Risk Analysis (ARA), 20/09/222, version 2.0, Status Final
19.	Email of the DPO dated 20.09.2022 on 4 tools used by Frontex Media Monitoring Team

20.	List of documents Themis 2021 and 2022 verified
21.	List of documents Focal Points Air
22.	2022_Weeks 33-34_BIWAR JO Themis 2022 : JO THEMIS 2022 - BIWEEKLY ANALYTICAL REPORT - 15–28 August 2022 (weeks 33-34)/SAMD/RAU/2022 - Ref. Ares(2022)6240421 - 09/09/2022)
23.	2022 Week 36 WAO JO Themis 2022 : FRONTEX CENTRAL MED-Analytical overview - 5-11 Sept 2022 (week 36) Ref. Ares(2022)6373064 - 15/09/2022
24.	2022 Week 35 WAO JO Themis 2022 : FRONTEX CENTRAL MED-Analytical overview - 29 Aug- 4 Sep (week 35) - Ref. Ares(2022)6214988 - 08/09/2022
25.	2022 JO Focal Points biweekly report 15.pdf : BI-WEEKLY ANALYTICAL UPDATE - Joint Operation FOCAL POINTS Air 2022 (Report 15: 11 August - 24 August 2022) - Ref. Ares(2022)6463598 - 19/09/2022
26.	2022_JO_Focal_Points_biweekly_report_14.pdf : BI-WEEKLY ANALYTICAL UPDATEJoint Operation FOCAL POINTS Air 2022 (Report 14: 28 July - 10 August 2022) - Ref. Ares(2022)6463317 - 19/09/2022
27.	2022 JO Focal Points biweekly report 13.pdf : BI-WEEKLY ANALYTICAL UPDATEJoint Operation FOCAL POINTS Air 2022(Report 12: 14 July - 27 July 2022) - Ref. Ares(2022)5706758 - 11/08/2022
28.	Specific Activity Plan - JO Focal Points Air 2022, Warsaw, signed on 24.01.2022
29.	Specific Activity Plan - Amendment no. 1- JO Focal Points Air 2022 (Ref. Ares(2022)5629414 - 08/08/2022)
30.	Operational Plan General Part - Multipurpose operational activities in the Member States (MOA-MS), Warsaw 14.12.2021, signed on 24.01.2022 (Reg. no. 13946/2021)
31.	Contact Details- JO Focal Points Air 2022
32.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air – BULGARIA, Warsaw, December 2021
33.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air – BELGIUM, Warsaw, December 2021
34.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –AUSTRIA, Warsaw, December 2021
35.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –THE NETHERLANDS, Warsaw, December 2021
36.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –SWITZERLAND, Warsaw, December 2021
37.	Logistical arrangements including information on working

	conditions - Joint Operation Focal Points Air –SPAIN, Warsaw, March 2022
38.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –SLOVENIA, Warsaw, December 2021
39.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –SPAIN, Warsaw, March 2022
40.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –SLOVAKIA, Warsaw, April 2022
41.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –ROMANIA, Warsaw, December 2021
42.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –PORTUGAL, Warsaw, June 2022
43.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –POLAND, Warsaw, December 2021
44.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –NORWAY, Warsaw, 27 April 2022
45.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –MALTA, Warsaw, not dated
46.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –LITHUANIA, Warsaw, December 2021
47.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –LATVIA, Warsaw, December 2021
48.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –ITALY, Warsaw, April 2022
49.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –ICELAND, Warsaw, December 2021
50.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –GREECE, Warsaw, December 2021
51.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –GERMANY, Warsaw, December 2021
52.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –FRANCE, Warsaw, December 2021
53.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –FINLAND, Warsaw, December 2021

54.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –ESTONIA, Warsaw, December 2021
55.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –DENMARK, Warsaw, December 2021
56.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –CZECH REPUBLIC, Warsaw, December 2021
57.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –CYPRUS, Warsaw, December 2021
58.	Logistical arrangements including information on working conditions - Joint Operation Focal Points Air –CROATIA, Warsaw, May 2022
59.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - AUSTRIA - Version September 2021
60.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - FRANCE (no date)
61.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - FINLAND - Version 5 January 2022
62.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - ESTONIA - Version 5 January 2022
63.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - DENMARK - Version November 2021
64.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - CZECH REPUBLIC - Version September 2021
65.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - CYPRUS (no date)
66.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - CROATIA - Version 5 January 2022
67.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - BULGARIA - Version 5 January 2022
68.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - BELGIUM (no date)
69.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - THE NETHERLANDS - Version September 2021
70.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - SWITZERLAND - Version September 2021
71.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - SPAIN (no date)

72.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - SLOVENIA - Version September 2021
73.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - SLOVAKIA - Version 5 January 2022
74.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - ROMANIA - Version 5 January 2022
75.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - PORTUGAL - Version 5 January 2022
76.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - NORWAY - Version 5 January 2022
77.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - MALTA- Version September 2021
78.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - LITHUANIA - Version 5 January 2022
79.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - LATVIA - Version 5 January 2022
80.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - ITALY (no date)
81.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - ICELAND - Version June 2022
82.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - GREECE - Version 5 January 2022
83.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - GERMANY - Version September 2021
84.	Specific Activity Plan JO THEMIS 2022, Warsaw, 14/12/2021, Reg. no. 13937/2021
85.	Logistical arrangements, including information on working conditions - JO Themis / Italy, Warsaw 14/12/2021
86.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - ITALY, Warsaw 14/12/2021
87.	Contact Details JO Themis 2022
88.	PeDRA transmissions from Terra and Themis during August 2021 - July 2022
89.	Agreement on Operational Cooperation between the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union

	(“FRONTEX”) and the European Police Office (“EUROPOL”), 4 December 2015
90.	Memorandum of understanding between Frontex and Eurojust, 18 December 2013
91.	Producing cases for onward transmission to Europol, Warsaw 31 May 2016
92.	Specific Activity Plan Amendment no 3 - Joint Operation TERRA 2022 - (Reg. No 13941C/2022)
93.	Contact Details and Available Databases JO Terra 2022 FOCAL POINTS - POLICE AND CUSTOMS COOPERATION CENTERS (PCCCs) INFORMATION EXCHANGE FRAMEWORK - Warsaw, 21 January 2022
94.	Contact Details JO TERRA 2022 - Warsaw, 22 August 2022
95.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - ESTONIA - Warsaw, 05 September 2022
96.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - BULGARIA - Warsaw, 26 August 2022
97.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - SLOVAKIA - Warsaw, 19 January 2022
98.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - ROMANIA - Warsaw, 30 June 2022
99.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - POLAND - Warsaw, 19 January 2022
100.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - NORWAY - Warsaw, 19 January 2022
101.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - LATVIA - Warsaw, 12 July 2022
102.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - LITHUANIA - Warsaw, 19 January 2022
103.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - HUNGARY - Warsaw, 19 January 2022
104.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - CROATIA - Warsaw, 19 January 2022
105.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - GREECE - Warsaw, 19 January 2022
106.	Logistical arrangements, including information on working conditions - Joint Operation Terra 2022 - FINLAND - Warsaw, 19 January 2022

107.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - ESTONIA - Version 05 January 2022
108.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - FINLAND - Version 05 January 2022
109.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - GREECE - Version 05 January 2022
110.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - SLOVAKIA - Version 05 January 2022
111.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - ROMANIA - Version 22 March 2022
112.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - POLAND - Version 05 January 2022
113.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - LATVIA - Version 05 January 2022
114.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - LITHUANIA - Version 05 January 2022
115.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - HUNGARY - Version 05 January 2022
116.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - CROATIA - Version 05 January 2022
117.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - BULGARIA - Version 05 January 2022
118.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - NORWAY - Version 05 January 2022
119.	Specific Activity Plan JO POSEIDON 2022 - Warsaw, 14/12/2021 - Reg. no. 13947/2021
120.	Contact Details JO Poseidon 2022 UPDATED on 08/09/2022
121.	Description of the tasks and specific instructions to the members of the teams including rules on use of force - GREECE (no date)
122.	Logistical arrangements, including information on working conditions 2JO Poseidon / Greece, Warsaw, 20/09/2021
123.	JORA JavaScript-HTML5 Business Case 1.1
124.	JEVO-Backlog.pdf - corrupted file
125.	JEVO-DevelopersReference.pdf- corrupted file

126.	JEVO Product Management
127.	JEVO technical design document
128.	JEVO Test Plan
129.	JEVO Test Report v2.77
130.	JORA2 Deployment procedure
131.	JORA2 Administration Manual
132.	JORA2 Administration Manual Incident
133.	JORA2 Administration Manual Intelligence
134.	JORA2 Administration Manual Interview
135.	JORA Business Case 2020
136.	PeDRA Business Case for PDPs to Europol
137.	PeDRA Business Case v4
138.	PeDRA Business Requirements Document
139.	PeDRA Technical Proposal (JORA)
140.	Procurement request JORA 2022
141.	TEST Run Application Layer Unit-Tests

Annex 3 Documents collected during the audit

1.	Incident report	Incident report FP Air n°322439 - Ref. 322439
2.	Incident report	Incident report FP Air n°316019 - Ref. 316019
3.	Debriefing interview	Interview report n°10781
4.	Report	Operationalisation of Common Risk Indicators v. 2021
5.	Public document	Strategic risk analysis 2022
6.	Debriefing interview	Interview report n°10787 - for legality check

7.	Debriefing interview	Interview report n°10769 - accepted
8.	Debriefing interview	Interview report n°10640 - accepted
9.	Debriefing interview	Interview report n°10771
10.	Debriefing interview	Interview report n°10614 - accepted
11.	email	Extracts from FRO monitoring report from Mission in Lesvos-Greece from 28 February to 10 March 2022
12.	Guidelines	JORA INCIDENT TEMPLATE GUIDELINES for AIR Operations
13.	Guidelines	JORA INCIDENT TEMPLATE GUIDELINES – LAND Operations
14.	Guidelines	JORA INCIDENT TEMPLATE GUIDELINES – SEA Operations
15.	Interview report	FRONTEX - Interview report no. 9962
16.	Interview report	FRONTEX - Interview report no. 9708
17.	Interview report	FRONTEX - Interview report no. 9975
18.	Interview report	FRONTEX - Interview report no. 10153
19.	Interview report	FRONTEX - Interview report no. 10217
20.	Interview report	FRONTEX - Interview report no. 10022
21.	Interview report	FRONTEX - Interview report no.10701
22.	Statistics (excel sheet)	No of transmissions from Terra and Themis during Aug 2021-July 2022
23.	Statistics (excel sheet)	FRONTEX-EUROPOL transmissions since Jan-2022.xlsx
24.	Decision	Decision of the Executive Director No R-ED -2021-25 adopting the ICT Cybersecurity Action Plan 2020-2025 of

		02/02/2021 Reference: ICT/ 887009 /2020
25.	E-mail	RE: [urgent] EDPS request - description of security incidents in IT-systems (operational personal data)
26.	Note	DeepL Pro brief security analysis
27.	Email including an attachment (word document)	1) Email to Fabrice Leggeri - Date: 2 June 2020 - Subject: Personal data breach policy 2) Word document EBCG Teams access to Schengen Information System (A2SISII) - Data Protection breach plan
28.	Word document	Personal data breaches Ref: HowTo/DataProtectionOffice/DPO/4/2022

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

1.	PowerPoint presentation	The concept of screening and debriefing
2.	PowerPoint presentation	PeDRA short overview
3.	PowerPoint presentation	Briefing on Targets : Present and Emerging trends at Air Borders - General Briefing- Air Borders 2021 AKA - New FTF ppt
4.	Screenshot	FRONTEX - Interview report no. 9708 - screenshot
5.	Interview report	FRONTEX - full Interview report no. 10701
6.	Attachments to report	FRONTEX - Interview report no. 9975 - Attachments
7.	Email	Date: 01/02/2022 To: Ntanouta.Paschopoulou Subject: PeDRA training for non-SC individuals involved in interview reporting/validation
8.	Email	Date: 25/02/2022 To: Pedra, HUMINT.OPA Subject: FW: JORA instructions for new colleagues
9.	Email	Date: 17/03/2022 To: klaus hudernigg,Alfonso Virone Subject: RE: JO Albania interviews processed by PeDRA
10.	Email	Date: 02/03/2022 To: Evangelos Mokalis, Marius Miklos, Piotr Kulesza Subject: RE: Pedra Team Guidelines
11.	Email	Date: 20 October 2022 - 13:49 To: Magdalena Nowacka Subject: RE: documents requested by the EDPS
12.	Excel sheet	FRONTEX-EUROPOL transmissions since Jan- July 2022.xlsx
13.	Email	Date: 07/10/2022 To: Vitor Bernardo, Andy Goldstein Subject: FW: Additional documents (request of Team C)
14.	PDF	Date: 13/10/2022 JORA Architecture
15.	PDF	Date: 13/10/2022 JORA Data Protection

16.	PDF	Date: 13/10/2022 JORA Product Management
17.	Word document	Date: 13/10/2022 EBCG teams access to Schengen Information System (A2SISII) Data Protection Breach Plan
18.	PDF	Date: 13/10/2022 DeepL Pro brief security analysis
19.	PDF	Date: 13/10/2022 DIG Unit presentation for EDPS Part1
20.	PDF	Date: 13/10/2022 DIG Unit presentation for EDPS part2
21.	Email	Date: 02/06/2022 To: Fabrice Leggeri Subject: Personal Data breach policy
22.	PDF	Date: 13/10/2022 ICT Cybersecurity Action Plan 2020-2025
23.	PDF	Date: 13/10/2022 Personal Data Breaches
24.	Email	Date: 07/10/2022 To: Bela Vonnak Subject: [urgent] EDPS request - description of security incidents in IT-systems (operational personal data)
25.	PowerPoint presentation	DIG presentation to EDPS on state of selected applications (Part 1)
26.	PowerPoint presentation	DIG presentation to EDPS on state of selected applications (Part 2)
27.	PowerPoint presentation	JORA Architecture - EDPS audit - 5-6 October
28.	PowerPoint presentation	JORA Data Protection - EDPS audit - 5-6 October
29.	PowerPoint presentation	JORA Product management - EDPS audit - 5-6 October

Annex 5 List of abbreviations

DbR	Debriefing Report
DO	Debriefing Officer
CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EBCG	European and Border coast Guard
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EIBM	European Integrated Border Management
FTF	Foreign Terrorist Fighters
FRO	Fundamental Right Officer
FRAN	Frontex Risk Analysis Network
FROM	Fundamental Right Officer Monitor
FSC	Frontex Situation Centre
ICC	International Coordination Centre
IO	Intelligence Officer
JO	Joint Operation
LCC	Local Coordination Centre
MB	Management Board
MRCC	Maritime Rescue Coordination Centre
MS	Member State
NCC	National Coordination Centre
OA	Operational Analyst
OP	Operational Plan
PeDRA	Processing of Personal Data for Risk Analysis
RAU	Risk Analysis Unit
SAP	Specific Activity Plan
TFEU	Treaty of the Functioning of the European Union