EUROPEAN DATA PROTECTION SUPERVISOR

AUDIT REPORT ON THE EUROPEAN BORDER AND COAST GUARD AGENCY (FRONTEX)

Warsaw, 5 and 6 October 2022 - EDPS Case number 2022-0749

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

[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.

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 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.

24 May 2023