



EUROPEAN DATA PROTECTION SUPERVISOR

**EDPS DECISION CONCERNING THE
INVESTIGATION
ON THE EUROPEAN BORDER AND COAST
GUARD (FRONTX) COMPLIANCE WITH
ARTICLE 71(1)(C) OF REGULATION (EU)
2018/1725 AND ARTICLE 90(2)(A) OF
REGULATION (EU) 2019/1896
(Case 2023-0537)**

**EUROPEAN
DATA
PROTECTION
SUPERVISOR**

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50



Contents

1. Scope	3
2. The investigative actions.....	3
3. Establishment of facts.....	6
3.1. Evolution of Frontex transmissions of operational personal data to Europol	6
3.2. Transmissions of operational personal data under the EBCG Regulation until 28 May 2023	8
3.3. Transmissions of operational personal data as from 29 May 2023.....	10
3.4. Onsite checks at Europol premises	11
3.5. Concept Note	12
4. Legal Assessment.....	13
4.1. Legal framework.....	13
The EBCG Regulation	13
4.2. Legal assessment.....	17
4.2.1. Processing of operational personal data by Frontex	17
4.2.2. Transmissions carried out between 4 December 2019 and 28 May 2023	18
4.2.3. Transmissions carried out as from 29 May 2023.....	23
4.2.4. Resuming transmissions on the basis of the concept note.....	23
5. Findings	24
6. Use of corrective powers	24

The European Data Protection Supervisor (the ‘EDPS’),

Having regard to the Treaty on the functioning of the European Union,

Having regard to Article 57(1)(f) and Article 58(2)(b) of Regulation (EU) 2018/1725 ¹,

Has adopted the following decision:

1. Scope

1. This document sets out the results on the investigation on whether Frontex has complied with Article 71(1)(c) of Regulation (EU) 2018/1725 and Article 90(2)(a) of Regulation (EU) 2019/1896² (the ‘EBCG Regulation’). While Article 90(2)(a) provides for the possibility for Frontex to exchange operational personal data with Europol or Eurojust, this investigation is limited to the transmission by Frontex to Europol of operational data contained in ‘debriefing reports’, i.e. the record of the debriefing interviews conducted by Frontex and/or national authorities of persons having irregularly crossed EU borders.
2. This Decision is addressed to Frontex.

2. The investigative actions

3. On 5 and 6 October 2022, the EDPS conducted an audit at Frontex Headquarters in Warsaw, Poland (the ‘2022 audit’). One of the topics of the audit was the processing of operational data by Frontex and its further transmission to the European Union Agency for Law Enforcement Cooperation (Europol) under Article 90(2) of the EBCG Regulation.

¹ [Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC; OJ L 295, 21.11.2018, p. 39–98. References to Articles in this document refer to the Regulation.

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.

4. On 24 May 2023, the EDPS communicated the audit report to Frontex.³ Findings 21 and 22 of the EDPS Audit Report ⁴ indicated that Frontex transmitted to Europol personal data collected during debriefing interviews about persons suspected to be involved in cross-border crimes without performing a strict necessity assessment of such transmissions and on a systematic basis, contrary to the requirements of Article 71(1)(c) of Regulation (EU) 2018/1725 and Article 90(2)(a) of the EBCG Regulation.
5. On 29 May 2023, following the findings of the EDPS audit report, Frontex decided to stop the transmission of debriefing reports to Europol.
6. On 9 June 2023, the EDPS decided to open an investigation and requested from Frontex the following documents/information:
 - Guidelines/documents/instructions/decisions detailing the conditions and procedure to be complied with by Frontex before sending operational personal data to Europol,
 - The last ten debriefing reports containing operational personal data that were sent to Europol by the date of the letter opening the investigation and the necessity assessment carried out by Frontex for each of them prior to their sending to Europol.
7. On 7 July 2023, Frontex provided the documentation requested.
8. In order to inform his understanding of the further processing by Europol of operational data received from Frontex and to assess the proportionality of the potential exercise of his corrective powers, the EDPS decided to conduct onsite checks at Europol premises. In order to prepare for the onsite checks, the EDPS requested Europol to provide the following information, which Europol provided by email on 27 September 2023:
 - Europol's guidelines/documents/instructions (if specific) detailing the procedures of receiving data from Frontex and processing them. If no specific documentation exists, the general procedures followed;
 - Europol's feedback to Frontex regarding the personal data received via debriefing interviews for the years 2020, 2021, 2022 (if available);
 - Europol's statistics/information regarding the use of personal data received by Frontex via debriefing interviews for the years 2020, 2021, 2022 (e.g. - how many entities were created on the basis on these data, (including breakdown per Data

³ EDPS Audit Report of 24 May 2023 on the audit carried out at Frontex on 5 and 6 October 2022.

⁴ EDPS Audit Report of 24 May 2023, p. 59.

- Subject Category), in how many intelligence reports the data were used, to what extent personal data from debriefing reports is transmitted to third parties);
- Europol's statistics concerning the total number of Frontex debriefing reports currently stored at Europol; The working arrangement between Frontex and Europol regarding the exchanges of personal data.
9. On 4 October 2023, the EDPS conducted the onsite checks at Europol premises.
 10. On 31 October 2023, the EDPS provided by letter draft minutes of the onsite checks to Europol. Europol submitted their comments on 16 November 2023.
 11. On 21 November 2023, the Frontex Deputy Executive Director for Information Management and Processes informed the EDPS orally that the Agency had resumed these transmissions of debriefing reports to Europol on a case-by-case basis.
 12. The EDPS sent the final set of minutes of the onsite checks to Europol on 15 December 2023, of which Europol acknowledged good receipt on 21 December 2023.
 13. On 4 January 2024, the EDPS requested additional information from Frontex:
 - the date when the transmission of the debriefing reports to Europol resumed;
 - the criteria used to conduct the strict necessity assessment of the exchange of operational personal with Europol ;
 - the document where these criteria are provided for;
 - The number of debriefing reports received by Frontex's PeDRA team analysts from all ongoing joint operations since the transmissions resumed and the number of debriefing reports actually transmitted to Europol;
 - The first debriefing report of every five debriefing reports transmitted to Europol since the transmissions resumed;
 - The respective strict necessity assessment carried out for each of the abovementioned reports with an explanation on how the criteria were applied. Where relevant, the related documents that have been used to assess the strict necessity of the transmission (e.g. request from Europol).
 14. On 22 January 2024 Frontex provided its reply⁵.

⁵ Letter of the Deputy Executive Director of Frontex for Administration and Information Management of 19 January 2024.

15. On 18 July 2024, the EDPS issued a preliminary assessment to provide Frontex with the opportunity to submit observations, in particular on the facts mentioned in the preliminary assessment, before any possible enforcement actions. Considering that the potential infringement by Frontex of Article 90 (2) (a) of the EBCG Regulation identified by the EDPS in his preliminary findings has an impact on Europol, the EDPS also provided Europol with the opportunity to submit its observations on the preliminary assessment.
16. On 30 September 2024, Frontex replied to the EDPS' preliminary assessment.
17. On 3 October 2024, Europol replied to the EDPS' preliminary assessment.
18. The EDPS has carefully assessed Frontex and Europol comments on the preliminary assessment and has taken these comments into account in his decision.

3. Establishment of facts

3.1. Evolution of Frontex transmissions of operational personal data to Europol

19. On 15 April 2015, Frontex submitted a notification for prior checking to the EDPS⁶ relating to the operational project Processing of Personal Data for Risk Analysis ('PeDRA') on the basis of Article 11c of Regulation 2007/2004.⁷ PeDRA, which was launched in 2016, consists in collecting information about suspects through the interviews of migrants intercepted at the external borders of the Union (so called 'debriefing interviews'). At that time, the interviews were conducted by the competent Member State authorities (without Frontex involvement), which then forwarded the information to Frontex on the initiative of the transmitting Member State. Frontex then

⁶ Opinion on a notification for Prior Checking received from the Data Protection Officer of Frontex regarding the Processing of Personal Data for Risk Analysis (PeDRA) (Case 2015-0346).

⁷ Council Regulation 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, pp 1-11 as amended by Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending 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 304, 22.11.2011, pp.1-17.

conducted a legality check of the information received. Personal data that passed the legality check were stored in Frontex's databases. Then Frontex processed them to form:

- Personal Data Packages that were transmitted to Europol and,
 - Risk analyses (the results of which do not include personal data) which were disseminated to regular consumers of Frontex risk analysis products.
20. PeDRA was the first operational step to allow Member States to transmit in a secure manner to Frontex personal data collected during or in the context of Frontex coordinated operational activities, and for Frontex to develop a system to further process the personal data to produce and transmit Personal Data Packages containing personal data to Europol on a case-by-case basis.⁸
21. In his Opinion of 3 July 2015⁹ regarding a prior check by Frontex on PeDRA, the EDPS stressed 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. The EDPS stressed 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.
22. On 18 December 2015, following the EDPS' Opinion, the Management Board of Frontex adopted Decision No 58/2015 on implementing measures for processing of personal data collected during Joint Operations, pilot projects and rapid interventions ('MB Decision 58/2015')¹⁰. This MB Decision established criteria for Frontex to evaluate the necessity of the transmission of personal data to Europol.
23. On 4 December 2015, Frontex concluded an operational agreement with Europol, in order to establish cooperative relations between Europol and Frontex through the

⁸ PeDRA Business Case 6.0, Warsaw, September 2015, File n°: (6.0)

⁹ Opinion of 3 July 2015 on a notification for Prior Checking received from the Data Protection Officer of Frontex regarding the Processing of Personal Data for Risk Analysis (PeDRA) – (Case 2015-0346).

¹⁰ 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.

exchange of information including the transmission of personal data by Europol to Frontex.

24. On 18 October 2016, following the adoption of Regulation 2016/1624 of 14 September 2016¹¹, Frontex informed the EDPS - through an update of its notification for prior checking relating to PeDRA - about its intention to deploy members of its own staff to assist Member States in the collection of personal data about suspects through conducting debriefing interviews of migrants intercepted at the external borders of the Union on the basis of Article 47 (1) of this Regulation. This provision allowed Frontex to process personal data about persons suspected, on reasonable grounds, by the Member State's competent authorities, of involvement in cross-border crime and transmitted to it by the Member States or by its own staff in the context of joint operations, pilot projects and rapid border interventions, and by migration management support teams where transmission to EASO, Europol or Eurojust is necessary for use in accordance with their respective mandates and within the framework of a working arrangement.
25. In its reply of 24 November 2016, the EDPS concluded that he had no recommendations as regards this update.

3.2. Transmissions of operational personal data under the EBCG Regulation until 28 May 2023

26. On 4 December 2019, Regulation (EU) 2019/1896 (the 'EBCG Regulation') repealed Regulation 2016/1624. Article 90 of the EBCG Regulation now explicitly allows Frontex to process operational personal data, which 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 in accordance with Chapter IX of Regulation (EU) 2018/1725. Article 90(2) (a) authorises Frontex to exchange these data with Europol where 'strictly necessary' for the performance of Europol's mandate and in accordance with Article 68.
27. During the 2022 audit, the EDPS audited the compliance with Article 90 EBCG Regulation and in particular, the transmission of operational personal data from Frontex to Europol. The EDPS found that, as of the entry into force of the EBCG Regulation,

¹¹ 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, 16.09.2016, pp.1-76

Frontex did not carry out the strict necessity assessment required by Article 90 (2) (a) of the EBCG Regulation, before sharing personal data about individuals suspected to be involved in cross-border crime with Europol.¹²

28. In particular, the EDPS found that Frontex’s debriefing officers deployed in the host Member State collect information about suspects of illegal immigration, human smuggling or other cross-border criminal activities mentioned by the interviewees. This information is included in a so-called “debriefing report” drafted by Frontex officers on the basis of the interview. The debriefing report is inserted in the Joint Operation Reporting Application (‘JORA’) and is sent further to the host Member for verification. Once validated, it is then shared with Frontex’s PeDRA team analysts at Frontex headquarters. Frontex’s analysts verify that these reports do not contain other personal data than those related to suspects of cross-border crimes and that the personal data contained in the reports are put between square brackets. Each interview report including its attachments is then transmitted to Europol using the Secure Information Exchange Network Application (SIENA) in the form of a personal data package (one SIENA message per report). During the audit, the PeDRA team analysts informed the EDPS that they 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.¹³ As a consequence and given the lack of assessment, no further documentation could be requested/checked.
29. By letter of 7 July 2023, Frontex contended¹⁴ that they assess the necessity of transmitting the debriefing reports containing operational personal data to Europol on a case-by-case basis, subject to the following criteria:
- The data is necessary for Europol to meet its objectives, as defined in Article 3 of Regulation (EU) 2016/794 (‘Europol Regulation’)¹⁵,

¹² Audit minutes, p. 25.

¹³ Audit minutes, p. 25.

¹⁴ Frontex reply of 7 July 2023.

¹⁵ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114 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, PE/8/2022/REV/1, OJ L 169, 27.6.2022, p. 1–42.

- The data subjects fall within the remits established by Article 18 and Annex II of the Europol Regulation,
 - The crime areas fall within the remits established by Annex I of the Europol Regulation.
30. Following an EDPS request¹⁶, Frontex communicated the ten last debriefing reports sent to Europol before Frontex decided to stop the transmission of debriefing reports to Europol on 29 May 2023. The last debriefing report was dated on 2 May 2023. Frontex indicated for each of these reports that *'the data are in line with Articles 3, 4, 18 of the Europol Regulation, as well as Annexes I and II'* as result of their necessity assessment.¹⁷ Frontex mentioned that these interviews contain exclusively personal data of migrants smugglers, which is necessary for the fulfilment of the Europol mandate and they were accepted by Europol.
31. Frontex further explained that they have no electronic record and that the assessment of the necessity to transmit the reports to Europol was created on the basis of a survey of Frontex staff. The EDPS understands from this explanation that Frontex requested its staff to assess and provide retroactively (i.e. after the transmission of the debriefing reports containing operational personal data to Europol) justifications on the necessity of the transmission of the operational personal data contained in the debriefing reports to Europol.

3.3. Transmissions of operational personal data as from 29 May 2023

32. As from 29 May 2023 and following the EDPS audit report of 24 May 2023, Frontex decided to interrupt the transmission of the debriefing reports to Europol.¹⁸
33. Since then, Frontex transmitted operational personal data to Europol in one single case (although they received two requests) on the basis of a specific and targeted request from Europol: on 27 June 2023, Europol requested Frontex to provide information, including operational personal data of suspects, to support the Greek authorities in investigating the criminal network involved in the smuggling of migrants on board of the fishing boat *Adriana* that sunk on 14 June 2023 where over 600 migrants died.¹⁹

¹⁶ EDPS letter of 9 June 2023.

¹⁷ See word document entitled 'last 10 interviews for EDPS' attached to Frontex letter of 7 July 2023.

¹⁸ Frontex briefing note of 03.07.2023 on Europol's request for assistance in the Pylos shipwreck case (SAMD/RAU).

¹⁹ Letter of 19 January of Frontex to the EDPS (ref. DED-IM/2023 - Ref. ARES(2024)439316) and SIENA_2163349-11-1_SOC.AP Migrant Sm._Request

Europol compiled a list of 11 incidents potentially relevant for the investigation in Greece and asked Frontex to assess its data sources and provide Europol with all available information, including debriefing interviews.²⁰ Frontex considered that Europol's request was sufficiently precise, targeted and linked to a specific ongoing criminal investigation of the Greek authorities which received the support of Europol, and thus decided to transmit the information requested, including debriefing reports containing operational personal data after a detailed assessment of the matching of each report with the criteria provided by Europol.²¹

34. On 27 September 2023, Frontex received another request from Europol, which it decided to reject. Europol was asking for information from a specific departure point in the Central Mediterranean, including operational personal data [REDACTED] to assess the level of involvement of organized criminality in migrant smuggling in the Central Mediterranean, with a view to complete the intelligence picture and potentially support the initiation of investigations into migrant smuggling networks.²² In her assessment, the Frontex DPO considered that to initiate a criminal investigation an event should occur that would give rise to suspicion of a criminal activity being committed. She concluded that in the absence of an ongoing criminal investigation and the lack of clarity about the necessity of collecting personal data on suspects to initiate a criminal investigation, the request lacked substantiation.²³ Therefore, Frontex rejected Europol's request, asking them to clarify to which task under Article 4 of Europol Regulation their request was relating to and to further justify the strict necessity for this transmission.²⁴

3.4. Onsite checks at Europol premises

35. The onsite checks carried out by the EDPS at Europol premises and the review of the documentation requested have shown that for the years 2020-2022:

²⁰ Frontex briefing note of 03.07.2023 on Europol's request for assistance in the Pylos shipwreck case (SAMD/RAU) and Europol Sienna Information Exchange Message, Request 2163349-11-1, dated on 27.06.2023.

²¹ Idem

²² SIENA_2163349-11-1_SOC.AP Migrant Sm._Request.

²³ Frontex DPO necessity and proportionality assessment of 23 October 2023 on Europol request from to share information on migrant smuggling on the Central Med route.

²⁴ Letter of 19 January of Frontex to the EDPS (ref. DED-IM/2023 - Ref. ARES(2024)439316)

- a) 4397 debriefing reports were transmitted by Frontex to Europol;
- b) these debriefing reports are processed in the Analysis Project Migrant Smuggling;
- c) on the basis of the above reports Europol processed data on 937 suspects and 29 contacts and used the data transmitted from Frontex in 875 intelligence reports;
- d) individuals should be fully identified [REDACTED] in order to be considered as person entities ;

- e) [REDACTED]
- f) [REDACTED]

3.5. Concept Note

- 36. On 21 November 2023, Frontex and Europol agreed on a Concept Note²⁵ which aimed at setting up the basis for the development of a governance model for the exchange of operational personal data, in accordance with the respective legal frameworks of both agencies. This concept note is considered by Frontex and Europol as a first step for the development of the negotiations to establish a new working arrangement.
- 37. The Concept Note distinguishes between two types of requests originating from Europol to Frontex: specific and targeted requests, and generic requests.
 - a) Specific and targeted requests should be in line with the rules defined in the Europol Regulation (handling codes and dissemination matrix). Namely, the request must originate from a relevant Analysis Project and Europol must indicate at least:
 - the relevant area of cross border crime,
 - the context of the request
 - the justification for the need to obtain this information.

²⁵ Concept Note on cooperation between Frontex and Europol regarding the exchange of information including operational personal data, Internal ref. SAMD/RAU/2023

b) Generic requests must originate from an Analysis Project and Europol must indicate ad minima:

- the relevant Analysis Project(s),
- the areas of cross-border crime,
- the data categories supported by the relevant Analysis Project(s).
- the context of its request, including the criminal intelligence needs and requirements based on which Frontex will perform the necessity assessment.

38. Furthermore, the Concept Note also provides for the possibility of Frontex to issue “Notifications” to Europol. In case Frontex identifies personal data deemed to be relevant to Europol’s mandate and which qualifies in terms of necessity and proportionality for transmission to Europol, Frontex should submit a notification with the same contextual information as specified above (for generic requests) to enable Europol’s assessment of the need to know according to Europol’s mandate. In such cases, Europol will provide Frontex, upon notification by the latter and before the exchange of operational personal data, with information that enables Frontex to assess the proportionality and necessity of the transmission of the case related operational personal data.

4. Legal Assessment

4.1. Legal framework

The EBCG Regulation

39. Article 90 (1) of the EBCG Regulation provides that where Frontex ‘*in the performance of its tasks under Article 10 (1) (q) processes personal data, which 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*’, it shall process such personal data in accordance with Chapter IX of Regulation (EU) 2018/1725. Furthermore, ‘*Personal data processed for that purpose (...) shall relate to natural persons whom the competent authorities of the Member States, Europol, Eurojust or the Agency have reasonable grounds to suspect are involved in cross-border crime. Such personal data may*

include personal data of victims or witnesses where those personal data supplement the personal data of suspects processed by the Agency in accordance with this Article.'

40. Pursuant to Article 10 (1) (q) of the EBCG Regulation, Frontex shall '*within the respective mandates of the agencies concerned, cooperate with Europol and Eurojust 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.*'
41. Under Article 90 (2) (a) of the EBCG Regulation Frontex shall only exchange the operational personal data with Europol where they are strictly necessary for the performance of Europol's mandate and in accordance with Article 68 of the same Regulation.
42. Under Article 68 (5) of the EBCG Regulation, any transmission of personal data by Frontex to other Union institutions, bodies, offices and agencies ('EUIBOA') must be subject to specific working arrangements regarding the exchange of personal data. These working arrangements must include a provision ensuring that personal data transmitted to EUIBOA by Frontex may be processed for another purpose only if authorised by Frontex and if compatible with the initial purpose for which the data were collected and transmitted by Frontex.
43. Article 86 (2) of the EBCG Regulation requires that the management board of Frontex adopts internal rules on the application of Regulation (EU) 2018/1725.
44. Such rules were adopted on 21 December 2021 in MB decision 69/2021 adopting the rules on processing operational personal data (the 'MB decision 69/2021'). Before the adoption of these rules, the MB decision 58/2015 of 18 December 2015 adopting implementing measures for processing personal data collected during joint operations, pilot projects and rapid interventions²⁶ ('MB decision 58/2015') remained applicable to the extent that it was not contradictory to the EBCG Regulation.
45. The MB Decision 58/2015 included a specific provision (Article 15) on the transfer of personal data to Europol. This provision listed the legal requirements of any transmission of personal data to Europol. It also required Frontex to make an evaluation of the necessity and proportionality of the transfer. This evaluation had to be based on information supplied in advance by Europol and listed in specific Operational Plans.

²⁶ MB Decision 58/2015 of 18 December 2015 adopting implementing measures for processing personal data collected during joint operations, pilot projects and rapid interventions, Reg. No.20906

46. 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 (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)).

47. 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 and for inclusion 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.

48. The MB decision 69/2021, applicable since 21 December 2021, lays down the rules on the application of Chapter IX of Regulation (EU) 2018/1725 regarding the processing of operational personal data in accordance with Article 90 of the EBCG Regulation.

49. As regards the exchange of operational personal data with Europol, Article 19 of MB decision 69/2021 provides that the transmission by Frontex of operational personal data must

- a) be performed only if the data are necessary for use in accordance with their respective mandates;
- b) be subject to specific working arrangements as stated in the second subparagraph of Article 68(5) of the EBCG Regulation;

- c) follow the *need to know* and *right to know* principles as stated in Article 18(3) of this Annex;
- d) respect the principles of necessity and proportionality; the Agency should only process personal data that are adequate and in their extent proportionate in relation to the purpose defined in Article 5 of the MB decision, i.e. for the purpose of identifying suspects of cross-border crime while performing its tasks under Article 10(1) (q) of the EBCG Regulation;

Article 19, last sentence states that the specific working arrangements referred to in point (b) will provide further details on the exchange of operational personal data between Frontex and Europol.

50. Pending the adoption of the specific working arrangement on the basis of Article 90 of the EBCG Regulation and Article 19 of the MB decision 69/2021, the agreement on operational cooperation concluded on 4 December 2015 between Frontex and Europol²⁷ (the ‘agreement of 4 December 2015’) remains applicable to the extent that it is not contradictory to the EBCG Regulation. This agreement provides safeguards such as the keeping by Frontex and Europol of records and reasons of transfers of personal data (Article 9(5)). It also states that Europol will provide Frontex with regular feedback on statistical information (e.g. the amount of data input into Europol systems, and number of hits generated) and a general overview of the further use of information received from Frontex (e.g. contributions resulting in new, or assisting ongoing investigations or joint investigation teams).²⁸

Regulation (EU) 2018/1725

51. According to Article 2(1) of Regulation (EU) 2018/1725, this Regulation applies to the processing of personal data by all Union institutions and bodies. Pursuant to the second paragraph of the same article, only Article 3 and Chapter IX of this Regulation applies to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU. Despite the fact that Frontex activities do not fall within the scope of these Chapters, Article 90(1) of the EBCG Regulation explicitly refers to the

²⁷ *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”), Brussels, 4 December 2015.*

²⁸ Article 18

application of Chapter IX of Regulation (EU) 2018/1725 for data processing activities carried out pursuant to Article 90 of the EBCG Regulation ('processing of operational data').

52. The concept of 'personal data' is defined in Article 3(1) of Regulation (EU) 2018/1725 as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier 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 natural person'.
53. Article 3(3) of Regulation (EU) 2018/1725 includes the definition of 'processing' which means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
54. Article 71 (1) (b) and (c) in Chapter IX of Regulation (EU) 2018/1725 requires that operational personal data are collected for specified, explicit and legitimate purposes ('purpose limitation') and are adequate, relevant and not excessive in relation to the purposes for which they are processed ('data minimisation'). Pursuant to Article 71 (4) of the same Regulation, the controller must be able to demonstrate compliance with Article 71 (1) (b) and (c).
55. According to Article 74 (3) of Regulation (EU) 2018/1725, in case it emerges that incorrect operational personal data have been transmitted or that operational personal data have been unlawfully transmitted, the recipient should be notified without delay. In such a case, the operational personal data concerned should be rectified or erased or their processing should be restricted in accordance with Article 82 of Regulation (EU) 2018/1725.

4.2. Legal assessment

4.2.1. Processing of operational personal data by Frontex

56. During debriefing interviews, the debriefing officer collects information in the form of a narrative report about suspects of illegal immigration, human smuggling or other cross-border criminal activities mentioned by the interviewee. The debriefing officer

records this information in a debriefing report. Frontex officers insert the debriefing reports in the Joint Operation Reporting Application ('JORA') and send them further to the host Member for verification. Once validated, the debriefing reports are shared with Frontex's PeDRA team analysts at Frontex headquarters where analysts verify that these reports do not contain other personal data than those related to suspects of cross-border crimes and that the personal data contained in the reports are put between square brackets. Each debriefing report including its attachments is then transmitted to Europol using the Secure Information Exchange Network Application (SIENA) in the form of a personal data package (one SIENA message per report).

57. The information included in the 'debriefing reports' regarding suspects of illegal immigration, human smuggling or other cross-border criminal activities mentioned by the interviewees constitute personal data of these suspects as the latter are identifiable natural persons.
58. The different operations performed by Frontex over the data (collection, recording, storage, disclosure by transmission) constitute 'processing' of these data in line with the definition included in Article 3(3) of Regulation (EU) 2018/1725.
59. Frontex conducts debriefing interviews for two purposes:
 - (1) carrying out risk analysis on the basis of Articles 87 (1) (e) EBCG Regulation and,
 - (2) identifying suspects of cross-border crime in view of their further transmission to Europol (PeDRA) (processing of operational data) based on Articles 87 (1) (d) and 90 EBCG Regulation. Pursuant to Article 90 EBCG Regulation, the operational personal data processed in this context are subject to a specific set of data protection rules contained in Chapter IX of Regulation (EU) 2018/1725.

4.2.2. Transmissions carried out between 4 December 2019 and 28 May 2023

60. Article 71 (1) (c) in Chapter IX of Regulation (EU) 2018/1725 requires that operational personal data are adequate, relevant and not excessive in relation to the purposes for which they are processed ('data minimisation'). According to the case law of the Court of Justice of the European Union ('CJEU'), any processing of personal data must

imperatively comply with the data minimisation principle.²⁹ This is a fundamental requirement to be complied with in order to ensure the lawfulness of the processing.

61. The EDPS interprets Article 90 of the EBCG Regulation read in the light of the provisions defining 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 limiting Frontex's processing of personal data for the purposes of the fight against cross-border crime and terrorism to a strict role of support to Member States' law enforcement authorities and of cooperation with Europol and Eurojust within their respective mandates. Hence, Frontex may only process operational personal data that are strictly limited to identified needs of Europol, Eurojust and MS competent authorities.
62. Article (90) (2) (a) of the EBCG Regulation provides that Frontex may only exchange operational personal data with Europol when they are 'strictly' necessary for the performance of Europol's mandate and in accordance with Article 68 (i.e. subject to a specific working arrangement regarding the exchange of personal data, which must include a provision ensuring that personal data transmitted to EU institutions, offices, bodies and agencies by Frontex may be processed for another purpose only if authorised by Frontex and if compatible with the initial purpose for which the data were collected and transmitted by Frontex).
63. According to Article 71 (4) of Regulation (EU) 2018/1725, Frontex is responsible for compliance with this Regulation and must be able to demonstrate compliance with paragraphs 1, 2 and 3.
64. Under Article 26(1) of Regulation (EU) 2018/1725, which is also applicable for processing operations that fall within the scope of Chapter IX to the extent that there is no more specific provision included in this Chapter, 'the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'.
65. The EDPS notes that while Regulation 2016/1624 allowed Frontex to transmit personal data about suspects to Europol where 'necessary for use in accordance with Europol's mandate' (Article 47), the EBCG Regulation, which entered into force on 4 December 2019 and repealed Regulation 2016/1624, is more exacting as regards the conditions for

²⁹ See Case C-60/22 Bundesrepublik Deutschland, judgment of 4 May 2023, ECLI:EU:C:2023:373, paragraphs 57 and 65; Case C-511/18, 512/18, 520/18, La Quadrature du Net and Others, judgment of 6 October 2020, EU:C:2020:791, paragraph 208; Case C-439/18, Latvijas Republikas Saeima, judgment of 22 June 2021, EU:C:2021:504, paragraphs 96 and 98 and Case C-77/21, Digi, judgment of 20 October 2022, EU:C:2022:805, paragraphs 49 and 56.

such transmission: Under Article 90 (2) (a) of the EBCG Regulation the transmission must be done ‘only’ when ‘strictly necessary’ for the ‘performance’ of Europol’s mandate.

66. This ‘strict necessity’ requirement applicable to Frontex’s exchange of operational personal data with Europol under Article (90) (2) (a) of the EBCG Regulation constitutes a special form of implementation of the principle of data minimisation set out in Article 71 (1) (c) of Regulation (EU) 2018/1725 which must be observed by any data processing falling within this Regulation’s scope. In this way, further to the latest amendment of the EBCG Regulation, compliance with this special form of the data minimisation principle has become an integral part of the lawfulness of the processing operation consisting in the exchange with Europol of data about natural persons whom the competent authorities of the Member States, Europol, Eurojust, or the Agency have reasonable grounds to suspect are involved in cross-border crime.
67. The data minimisation principle should be read in the light of the purpose limitation principle set out in Article 71 (1) (b) of Regulation (EU) 2018/1725, which requires to assess whether the personal data processed are adequate, relevant and not excessive in relation to the purposes for which they are processed. According to the purpose limitation principle, such purpose should be specified, explicit and legitimate.
68. Under Article 68 EBCG Regulation, the purpose for which operational data are shared with Europol also defines the scope of the further processing by this Agency and the legitimacy of any further data sharing with third parties.
69. The CJEU clarified in its ruling in case C-205/21 of 26 January 2023 that the requirement of ‘strict necessity’ must be interpreted as establishing strengthened conditions for lawful processing of the data. It aims at giving enhanced protection with regard to the processing, which, because of the particular sensitivity of the data at issue and the context in which they are processed, is liable to create significant risks to fundamental rights and freedoms, such as the right to respect for private life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter.³⁰

³⁰ Case C-205/21, Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organizirana prestapnost, Judgment of 26 January 2023, ECLI:EU:C:2023:49, paragraphs 116 and 117.

70. The Court specifies that the use of the adverb ‘only’ before the words ‘where strictly necessary’ underlines that ‘the processing will be capable of being regarded as necessary solely in a limited number of cases’.³¹
71. In addition, the fact that the article refers to ‘strict’ necessity for processing of such data means that that necessity is to be assessed with particular rigor.³²
72. The Court also stresses that the purposes of processing cannot be indicated in terms that are too general, but have to be defined sufficiently precisely and specifically to enable assessment of whether that processing is ‘strictly necessary’.³³
73. Also in the light of that case law, the EDPS submits, that by raising the threshold in terms of lawfulness of the personal data processed and therefore strengthening the key principle of data minimisation, the legislator intended to give enhanced protection to individuals whose data were collected and further transmitted to Europol under Article 90 of the EBCG Regulation.
74. This means that, since 4 December 2019, for any transmission of operational personal data to Europol, Frontex must assess more rigorously whether Europol would strictly need these data to actually perform its mandate. It follows from these provisions that, since Frontex is authorised under Article 90(2)(a) of the EBCG Regulation to exchange operational data with Europol only when strictly necessary for the performance of its mandate in general, the Agency must perform a case-by-case assessment of whether each data transmitted is adequate, relevant and not excessive in relation to specified, explicit and legitimate purposes. Considering also that the specific purpose of the transmission will also serve to define the scope of further processing by Europol, a general reference to the mandate of Europol is thus excluded.
75. In addition, Frontex must be able to demonstrate such necessity in accordance with Article 71 (4) and 26 of Regulation (EU) 2018/1725. This responsibility encompasses ensuring that the strict necessity assessment as described above is properly documented and can be shared e.g. with the EDPS upon request.

³¹ Case C-205/21, Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organizirana prestapnost, Judgment of 26 January 2023, ECLI:EU:C:2023:49, paragraphs 117-118.

³² Case C-205/21, Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organizirana prestapnost, Judgment of 26 January 2023, ECLI:EU:C:2023:49, paragraph 118 read in light of paragraph 117 of the same ruling. See also paragraph 119.

³³ Case C-205/21, Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organizirana prestapnost, Judgment of 26 January 2023, ECLI:EU:C:2023:49, paragraphs 122 and 124.

76. Frontex's assessment for each debriefing report is limited to the indication that '*data contained therein are in line with Articles 3, 4, 18 of the Europol Regulation, as well as Annexes I and II*'. This assessment is far too broad to meet the requirement of strict necessity as interpreted by the Court: it results from the interpretation by the CJEU that the purposes of processing cannot be indicated in terms that are too general, but have to be defined sufficiently precisely and specifically to enable assessment of whether that processing is 'strictly necessary'.³⁴ In the case at hand, Frontex's assessment cannot be limited to a reference in general terms to the mandate, list of purposes for which Europol may process personal data, the list of crimes it is competent for, and the categories of data subjects about whom it is allowed to process personal data.
77. The EDPS also considers that the necessity criteria included in the MB Decision 58/2015 (i.e. the categories of data required from the operational area, the nationalities, areas of crime and geographical locations that are of current interest from the operational area), combined with the regular feedback that Europol should have provided to Frontex further to the Agreement of 4 December 2015 on statistical information (e.g. the amount of data input into Europol systems, and number of hits generated) and on the general overview of the further use of information received from Frontex (e.g. contributions resulting in new, or assisting ongoing investigations or joint investigations) could have provided a first evidence base for Frontex to conduct a strict necessity assessment, provided it is conducted in a sufficiently detailed and informative manner.
78. However, Frontex assessments regarding the transmission of the debriefing reports to Europol in no way rely on, or refer to such detailed information and they do not provide further explanations on why the operational personal data contained in each report are necessary to meet Europol's objectives nor do they mention the Europol's tasks and the specific purposes for which they are transmitted. Hence, they cannot be considered, in the EDPS view, as the particularly rigorous necessity assessment as required by Article 90(2)(a) .
79. Furthermore, the fact highlighted by Frontex that Europol has implemented a two-steps verification process of data protection compliance for all information received via SIENA (and thus also for operational personal data sent by Frontex to Europol) cannot substitute, in the EDPS's view, the *obligation of Frontex* to verify before sending operational personal data to Europol that these data are strictly necessary for Europol

³⁴ Case C-205/21, Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organizirana prestapnost, Judgment of 26 January 2023, ECLI:EU:C:2023:49, paragraphs 122 and 124.

to perform its mandate. The EDPS also stresses in this context that the EBCG Regulation requires a 'strict' necessity assessment, which according to the above mentioned CJEU case law (see points 69-72), implies a more rigorous assessment of the data minimisation principle.

80. In the case under consideration and taking into account all the evidence brought before him, the EDPS considers that Frontex has not provided any evidence demonstrating that, prior to the transmission of operational personal data to Europol, Frontex has assessed the strict necessity of such transmissions on the basis of established criteria.
81. Therefore, the EDPS is of the opinion that the lack of a strict necessity assessment by Frontex for the transmission of operational personal data to Europol is an infringement of Article 90 (2) (a) of the EBCG Regulation and of Article 71 (1) (c) of Regulation (EU) 2018/1725 that affects the lawfulness of the exchanges.
82. The EDPS is also of the opinion that the inability of Frontex to demonstrate that they have complied with Article 71 (1) (c) of Regulation 218/1725 is a breach of Article 71 (4) and 26 of the same Regulation.

4.2.3. Transmissions carried out as from 29 May 2023

83. As from 29 May 2023, only in one single case, debriefing reports have been sent by Frontex to Europol. The EDPS takes note that this case concerned a specific targeted request addressed by Europol to Frontex for the purpose of an ongoing Greek criminal investigation supported by Europol. It was based on a list of 11 incidents identified by Europol for which Europol asked Frontex to provide them with debriefing reports in line with these incidents. The EDPS finds that in this specific case, the criteria for the transmission of the debriefing reports to Europol have therefore been defined sufficiently precisely and specifically to enable the assessment of whether that processing is 'strictly necessary'.

4.2.4. Resuming transmissions on the basis of the concept note

84. On 21 November 2023, Frontex and Europol agreed on a concept note which aimed at setting up the basis for the development of a governance model for the exchange of operational personal data, in accordance with the respective legal frameworks of both agencies. The EDPS understands that this note is a basis for further detailed rules on the transmission of operational personal data by Frontex to Europol and a stepping stone for the establishment of a new working arrangement with Europol.

85. The EDPS considers that the concept note is a suitable foundation on which Europol and Frontex may rely on to *further develop* the criteria for exchanging operational data. However he stresses that the note could not be considered sufficient *in itself* to resume transmissions of operational personal data to Europol. The criteria provided therein, in particular with regard to generic requests from Europol (i.e. the Analysis Project(s) from which the request originates, the areas of cross-border crime, the data categories supported by the relevant Analysis Project(s) and the context of the request) are too broadly worded to allow for a meaningful ‘strict necessity’ assessment, as required by Article 90(2)(a) of the EBCG Regulation.

5. Findings

86. In conclusion, the EDPS has found that Frontex for the time period between 4 December 2019 and 28 May 2023 has unlawfully transmitted operational personal data collected during debriefing interviews about persons suspected to be involved in cross-border crimes with Europol as the strict necessity of such transmission to Europol in order to perform its mandate has not been assessed by Frontex.
87. This is an infringement of Article 90 (2) (a) of the EBCG Regulation and of Article 71 (1) (c) of Regulation (EU) 2018/1725.
88. The EDPS has also found an infringement of the accountability principle as envisaged in Article 71(4) and 26 of Regulation (EU) 2018/1725.

6. Use of corrective powers


89. Under Article 52(3) of Regulation (EU) 2018/1725, the EDPS is responsible for monitoring and ensuring the application of the provisions of the Regulation and of any other Union act granting protections to natural persons whose data are processed by EU institutions. To that end, the EDPS exercises the powers granted in Article 58 of the Regulation, including corrective powers under Article 58(2).
90. The following measures are without prejudice to any other or further action the EDPS might undertake.

91. The EDPS has decided to reprimand Frontex under Article 58 (2) (b) of Regulation (EU) 2018/1725 considering that a reprimand is an appropriate and necessary corrective measure. A primary purpose of the EDPS' power to issue a reprimand is to achieve a dissuasive effect and to make it clear to the Union agency concerned that it has infringed the Regulation.
92. In order to ensure that the exercise of his corrective powers is appropriate, necessary and proportional, the EDPS takes into account the severity of the provisionally identified breaches and the risks for the data subjects that it entails as well as the measures that Frontex has already undertaken to address these risks.
93. As evidenced by the onsite checks the EDPS carried out at Europol on 4 October 2023, data exchanged from the 4397 debriefing reports during the period under investigation has resulted in the processing by Europol of data on 937 suspects and 29 contacts in their operational systems, further supporting the drafting of 875 intelligence reports.
94. Frontex has interrupted the transmission of all debriefing reports after the issuance of the EDPS audit report (i.e. five days after the communication of the EDPS audit report to Frontex). Since then, only in one single case, debriefing reports have been sent by Frontex to Europol, in which case the criteria for the transmission of the debriefing reports have been defined sufficiently precisely and specifically to enable the assessment of whether that processing is 'strictly necessary'.
95. Frontex has engaged in discussions with Europol in order to define the criteria that would allow the transmissions to resume. These discussions have so far led to the adoption of a joint concept note between Frontex and Europol that would constitute the basis for further detailed rules on the transmission of operational personal data by Frontex to Europol.
96. Frontex is reviewing internal guidelines and processes and in this context has included in the document "PeDRA intake process", the requirement to assess the necessity of the transmission of the data to Europol with established criteria. This document defines the steps for collecting reporting, pre-processing, and performing the legality check of operational personal data via the debriefing interview template of the Joint Operations Reporting Application (JORA) and its transmission to Europol via the Secure Information Exchange Network Application (SIENA).
97. In addition, regarding the severity of the breach and the risks for data subjects who, although they may not be of interest for Europol, would nevertheless end up in their systems, the EDPS stresses that the processing of data about individuals in an EU law

enforcement database can have deep consequences on those involved. Without a proper implementation of the data minimisation principle and the specific safeguards contained in the EBCG Regulation, data subjects run the risk of wrongfully being linked to a criminal activity across the EU, with all of the potential damage for their personal and family life, freedom of movement and occupation that this entails. In this regard, the EDPS notes that for the years 2020-2022, 4397 debriefing reports were transmitted by Frontex to Europol.

98. Pursuant to Article 64 of the Regulation, an action against this decision may be brought before the Court of Justice, within two months of its notification, in accordance with the conditions laid down in Article 263 TFEU.

Done at Brussels

 Digitally signed by:
WOJCIECH RAFAŁ
WIEWIÓROWSKI (EUROPEAN
DATA PROTECTION SUPERVISOR)
Date: 2024-12-05 15:13:03 UTC