



EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION ON THE TRANSMISSION OF PERSONAL DATA BY THE [REDACTED] AGENCY TO THE [REDACTED] INTELLIGENCE AUTHORITIES (Case 2023-1231)

1. INTRODUCTION

1. This Supervisory Opinion relates to a consultation submitted by the [REDACTED] Agency ([REDACTED] or the Agency) in relation to a request received from the [REDACTED] Intelligence and Security Services [REDACTED] for the transmission of personal data.
2. [REDACTED] has received this request from the [REDACTED] to provide the **personal data of 145 participants** (last name, first name, name of their organisation) **invited to an event organised by the Agency**¹ focused on [REDACTED].
3. The EDPS issues this Supervisory Opinion in accordance with Articles 57(1)(g) and 58(3)(c) of Regulation (EU) 2018/1725², ('EUDPR').

¹ [REDACTED]

² Regulation (EU) 2018/1725 of the European Parliament and 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, pp. 39-98.

2. FACTS

2.1. Correspondence between [REDACTED] and the [REDACTED]

4. The initial written request from the [REDACTED] to [REDACTED] dates of 8 September 2023 and concerns the list of participants to the 'European [REDACTED] Days 2023' organised by the Agency. It was the first time that [REDACTED] received such a request from the [REDACTED].
5. The same day, [REDACTED] asked for clarifications on the reason for the [REDACTED] request and referred to data protection considerations regarding the personal data of visitors and exhibitors of that event.
6. In their reply of 12 September 2023, the [REDACTED] indicated that they are not subject to the General Data Protection Regulation (GDPR) and referred to "routine checks" regarding certain companies and individuals that they are following³.
7. On 18 September 2023, [REDACTED] requested complementary information from the [REDACTED] regarding the legal basis and their assessment of the necessity and proportionality of their request.
8. On 20 September 2023, the [REDACTED] replied to [REDACTED] by providing the following legal references and pointing to the, according to them, "low intrusiveness" of their request:
 - As regards the **legal basis** for the processing, the [REDACTED] refers to Articles [REDACTED] of the [REDACTED] law [REDACTED] governing intelligence and security services (the [REDACTED])⁴:
 - [REDACTED] on the **missions** of Intelligence Services [automated translation]⁵:

'The [REDACTED] has for mission:

1° to seek, analyse and process information relating to factors that influence or may influence national and international securit [REDACTED]

³ [REDACTED]

⁴ [REDACTED]

⁵ Emphasis added.

[REDACTED]

[REDACTED]

4° to carry out the safety investigations [REDACTED]

5° to seek, analyse and process information relating to the activities of the foreign intelligence [REDACTED] (...)'

- [REDACTED] on the activities performed by the [REDACTED] Intelligence Services [automated translation]⁶:

[REDACTED] Intelligence and security services may search, collect, receive and process information and personal data that may be useful for the execution of their missions and keep up-to-date documentation relating, inter alia, to events, groupings and persons of interest in the performance of their tasks.

[REDACTED] The information contained in the documentation must be linked to the purpose of the file and be limited to the resulting requirements.

§3. Intelligence and security services shall ensure the security of data relating to their sources and information and personal data provided by these sources. [REDACTED]

[REDACTED]

- Regarding **lawfulness**, the [REDACTED] refers to Articles [REDACTED] of the law of [REDACTED] on the protection of natural persons with regard to the processing of personal data (the '[REDACTED]')⁷, which define

⁶ Emphasis added.

⁷

[REDACTED]

the rules on the processing of personal data by the [REDACTED]. These provisions include rules on grounds for lawfulness of the processing, data protection principles, processing of special categories of personal data, data retention, data subject rights, obligations of the controller, security, register of processing and data protection officer.

- As to the **supervisory authority**, the [REDACTED] notes that Article [REDACTED] provides that, by way of derogation, the authority in charge of supervising the processing of personal data by the [REDACTED] is the [REDACTED]⁸ [REDACTED]).

9. On 28 September 2023, [REDACTED] requested further information from the [REDACTED] on the scope and subject of the investigation in question. In addition, for data minimization purposes, [REDACTED] proposed a "hit/no hit" approach, whereby the [REDACTED] could provide [REDACTED] with the names of the persons targeted, and the Agency would indicate whether or not these persons had participated in the event concerned.

10. On 18 October 2023, the [REDACTED] provided an analysis conducted by their legal department. This analysis does not refer to the data minimization approach suggested by [REDACTED], but essentially:

- Refers to Articles [REDACTED] as the **legal basis** for the request for transmission and the intended subsequent processing of the personal data requested.
- Reiterates the [REDACTED] view that such requests are, in view of the powers to collect information attributed to the [REDACTED], the **least intrusive means** regarding fundamental rights⁹;
- Notes that [automated translation]¹⁰ *"In this case, the [REDACTED] monitors events related to the interests of [REDACTED] [REDACTED] taking place on its territory in order to be able to collect the information necessary for the performance of its legal duties. 'Routine verification' means the*

⁸ [REDACTED]

⁹ « .. [REDACTED] ».

¹⁰ Emphasis added.

*service means that this application is part of this follow-up. The essence of the activity of an intelligence service is to be prospective, our objective being to detect, an early stage, phenomena likely to pose a threat to the interests of protect. Specifically: the list of participants obtained will be analysed and processed in accordance with the law, and confronted with existing data from the [REDACTED] databases. The interest of the [REDACTED] relates to persons with links to certain countries or certain specific entities, always of interest (or even a threat) to our missions. **This information being classified, we cannot be more explicit under the law of [REDACTED] on classification**”;*

- Reiterates that the [REDACTED] is **not subject to the GDPR** and that the authority in charge of supervising the processing of personal data by the [REDACTED] is the [REDACTED]. It contains commitments to deal with any personal data received in line with data protection principles;
- Argues that the requested transmission is in line with Article [REDACTED] of the [REDACTED] Data Protection Law, as it is **necessary for the performance of a task carried out in the public interest** linked to national security, namely the “*follow-up of phenomena or individuals likely to threaten the [REDACTED] [REDACTED] in connection with the [REDACTED], or activities of foreign intelligence services on [REDACTED]*” [automated translation];
- Highlights **professional secrecy obligations** for any collaborator of the [REDACTED].

3. LEGAL ASSESSMENT

11. The EUDPR is applicable to processing by the [REDACTED] in accordance with Article 2(1) EUDPR, since the [REDACTED] is a Union agency set up on the basis of [REDACTED] and therefore one of the “Union institutions and bodies” as defined in Article 3(10) EUDPR.

12. This is further confirmed by [REDACTED], providing that [REDACTED] is subject to the rules laid down in the EUDPR as successor to

¹¹ [REDACTED]

Regulation (EC) 45/2001: in line with Article 99 EUDPR, references to the repealed Regulation (EC) 45/2001 shall be construed as references to the EUDPR.

13. The transmission request concerns the participants' list for an event organised by █████ containing last name, first name and name of their organisation for 145 participants (visitors and exhibitors). Insofar as these pieces of information allow for the direct identification of natural persons, they are personal data in the sense of Article 3(1) EUDPR.
14. Pursuant to the definition provided in Article 3(3) EUDPR, the concept of 'processing of personal data' designates '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, ... storage, ... consultation, use, disclosure by transmission, dissemination or otherwise making available ...'. It follows that the production of the participants' list for the event by █████ and as well the requested disclosure of personal data by transmission, like the storage or otherwise making available of data, would constitute processing for the purposes of Article 3(3) EUDPR and, accordingly, falls within the scope of the EUDPR (see, in analogy, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 45).
15. The mere fact that a national measure is based on the purpose of protecting member States' national security cannot render EU law inapplicable and exempt an Union institution from their obligation to comply with Union law.¹²
16. Article 9 EUDPR is the main data protection provision to consider when assessing whether █████ can transmit information to the █████, i.e. a recipient established in the Union other than EUIs (Section 3.1). In addition, any processing should comply with all provisions of the EUDPR (Section 3.2). Finally, the Opinion will mention also the Protocol No 7 on the Privileges and Immunities of the European Union¹³ (Section 3.3).

3.1. Conditions for the transmission of personal data to the █████ (Article 9 EUDPR)

17. Article 9 EUDPR establishes that personal data shall only be transmitted to recipients established in the Union other than Union institutions and bodies under certain

¹² See, by analogy, CJEU, judgments of 4 June 2013, ZZ, C-300/11, EU:C:2013:363, paragraph 38 and the case-law cited; of 20 March 2018, *Commission v Austria* (State printing office), C-187/16, EU:C:2018:194, paragraphs 75 and 76; and of 2 April 2020, *Commission v Poland, Hungary and Czech Republic* (Temporary mechanism for the relocation of applicants for international protection), C-715/17, C-718/17 and C-719/17, EU:C:2020:257, paragraphs 143 and 170).

¹³ Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FPRO%2F07>.

conditions. In the case at hand, the request for transmission originates from the █████, a █████ authority in charge of the protection of national security, i.e. a recipient established in the Union other than Union institutions and bodies.

18. Under Article 9(1)(a) EUDPR, the █████ as such recipient would need to establish that the personal data requested are (i) necessary for (ii) the performance of a task carried out in the public interest or in the exercise of official authority¹⁴.

Performance of a task carried out in the public interest or in the exercise of official authority

19. The █████ referred to Articles █████ of the █████ Law on Intelligence Services as the legal basis for the request for transmission and the intended subsequent processing of the personal data requested. Under Article █████ of the █████ Law on Intelligence Services, “*Intelligence and security services may search, collect, receive and process information and personal data that may be useful for the execution of their missions and keep up-to-date documentation relating, inter alia, to events, groupings and persons of interest in the performance of their tasks.*”.
20. In addition, the █████ has brought forward that their request for transmission serves the performance of a task carried out in the **public interest linked to national security**, namely the “*follow-up of phenomena or individuals likely to threaten the █████ in connection with the █████, or activities of foreign intelligence services on █████*”.
21. The request to provide the personal data concerns participants invited to an event organised by █████ focused on █████. As it is within the tasks attributed to the █████, inter alia¹⁵, to “*seek, analyse and process information relating to any activity that threatens or could threaten... scientific and economic potential in relation to the actors, both natural persons and legal persons, which are active in defence-related economic and industrial sectors*”, this request thus falls within the █████ statutory remit under █████ law. The transmission by █████ to the █████ would thus take place for the performance of a task carried out in the public interest by the █████ and the request consequently meets the second criterion under Article 9(1)(a) EUDPR.

Necessity of the data transmission to perform █████ tasks

22. For the application of Article 9(1)(a), recital 28 EUDPR provides that when recipients established in the Union other than Union institutions and bodies would like to have

¹⁵ See Article █████ of the █████ Law on Intelligence Services.

personal data transmitted to them by Union institutions and bodies, those **recipients should demonstrate that it is necessary** to have the data transmitted to them for the performance of their task carried out in the public interest.

23. Regarding the first criterion under Article 9(1)(a) EUDPR (“necessity”), the [REDACTED] has argued that *“In this case, the [REDACTED] monitors events related to the interests of [REDACTED] and the [REDACTED] taking place on its territory in order to be able to collect the information **necessary for the performance of its legal duties**. ‘Routine verification’ means the service means that this application is part of this follow-up. The essence of the activity of an intelligence service is to be prospective, our objective being to detect, an early stage, phenomena likely to pose a threat to the interests of protect. Specifically: the list of participants obtained will be analysed and processed in accordance with the law, and confronted with existing data from the [REDACTED] databases. The interest of the [REDACTED] relates to persons with links to certain countries or certain specific entities, always of interest (or even a threat) to our missions.”*
24. The [REDACTED] has, however, not further specified the legal duties it refers to beyond the generalities establishing the performance of a task carried out in the **public interest linked to national security**, namely the *“follow-up of phenomena or individuals likely to threaten the [REDACTED] in connection with the [REDACTED], or activities of foreign intelligence services on [REDACTED]”*.
25. Regarding the link between these legal duties and the participants of the [REDACTED] event in question, the [REDACTED] rather highlights that *“This information being classified, we cannot be more explicit under the law of [REDACTED] on classification”*.
26. In addition, the reference to “routine checks” regarding certain companies and individuals that the [REDACTED] is following is very vague and not further circumscribed. The fact that this is the first time that [REDACTED] receives such a request, while they organise events on a regular basis, would make it seem questionable whether those checks are “routine” rather than targeted.
27. Based on the information available to the EDPS, the [REDACTED] has so far not sufficiently established under Article 9(1)(a) EUDPR the necessity of the transmission of the list of participants for the performance of the tasks carried out by the [REDACTED] in the public interest. The conditions for [REDACTED] to transmit the requested personal data under Article 9 EUDPR are not (yet) fulfilled.

28. In addition, the [REDACTED] has so far failed to specify an explicit and legitimate **purpose**¹⁶ of their request for transmission. Instead, as outlined in §25 above, regarding the link between the [REDACTED] legal duties and the participants of the [REDACTED] event in question, the [REDACTED] rather highlights that “*This information being classified, we cannot be more explicit under the law of [REDACTED] on classification*”. In this regard, the [REDACTED] is currently not able to assess the necessity and proportionality against a sufficiently ‘specified, explicit and legitimate purpose’¹⁷ of the request.
29. Furthermore, the mere affirmation by the [REDACTED] that their request for transmission would be less intrusive on data subjects’ fundamental rights than ‘other more intrusive’ methods that the [REDACTED] can implement in the framework of their legal powers is not only insufficient, but also not relevant in the context of the **proportionality** assessment to be carried out by [REDACTED].
30. In view of the above, the EDPS **deems necessary** that [REDACTED] ask the [REDACTED] to further substantiate the specific purpose of the transmission of the data at stake (list of participants to a specific event organised by [REDACTED]), and why such transmission is necessary for the [REDACTED] to perform their tasks and proportionate to the goal pursued.

3.2. Compliance with the other provisions of the EUDPR

31. The requirements of Article 9 EUDPR are supplementary to the conditions for lawful processing¹⁸. The EDPS notes that, under Articles [REDACTED] of the [REDACTED] Data Protection Law, the [REDACTED] has to comply with data protection rules while carrying out processing activities.
32. Therefore, before transmitting the requested personal data, [REDACTED] should also verify in particular whether the data transmission:
- is lawful under Article 5;
 - complies with the data protection principles of Article 4, in particular purpose limitation and data minimisation;
 - complies with the provisions on data subject rights (Articles 14 to 23).

¹⁶ Article 4(1)(b) EUDPR; a similar principle applies to the [REDACTED] under Article [REDACTED] of the [REDACTED] data protection law.

¹⁷ Article 4(1)(b) EUDPR; a similar principle applies to the [REDACTED] under Article [REDACTED] of the [REDACTED] data protection law.

¹⁸ See recital 28, last sentence EUDPR.

Ground for lawfulness under Article 5

33. ■ could possibly rely on Article 5(1)(a) EUDPR, provided that they can demonstrate that the data transmission is necessary for a task carried out by ■ in the public interest or in the exercise of official authority vested in the Agency.
34. If there were a specific legal obligation for ■ (for example in the Seat Agreement¹⁹) to transmit the categories of data at stake to the ■ intelligence authorities, ■ could also possibly rely on Article 5(1)(b) EUDPR.
35. However, without further information available to the EDPS, these remain a hypothetical possibilities at this stage.

Data minimisation

36. The EDPS takes note of ■ proposal of a "hit/no hit" approach, whereby the ■ could provide ■ with the names of the persons targeted, and the Agency would indicate whether or not these persons had participated in the event concerned.
37. The EDPS recommends that ■ further explore whether and how they could limit the amount of data communicated to the ■. They could for example ask that the ■ provide additional information as to the type of individuals/organisations they are targeting, so that ■ could remove from the list of participants the profiles that are not relevant for the ■.

Purpose limitation

38. As noted above (§25), the ■ is currently not able to assess whether the intended data processing is compliant with the data protection rules, and in particular the purpose limitation of a sufficiently 'specified, explicit and legitimate purpose'²⁰ against which ■ could assess the necessity and proportionality of the request. See §33 for the respective action the EDPS deems necessary.

Transparency / data subject rights

39. ■ should provide general and transparent information on the processing and comply with all the other data subject rights, unless they can apply a restriction in accordance with their internal rules under Article 25 EUDPR²¹. The EDPS notes that ■ can, subject to certain conditions described in the internal rules, restrict data

¹⁹ The Seat Agreement was not communicated to the EDPS.

²⁰ Article 4(1)(b) EUDPR; a similar principle applies to the ■ under Article ■ of the ■ Data Protection Law.

²¹ ■

subject rights “to safeguard the national security, public security and/or defence of the Member States” in relation to personal data exchanged with competent authorities of the Member States²².

40. █████ internal rules on restrictions²³ indicate that █████ shall include in the data protection records, made available on their website, information relating to the potential restriction of data subject rights and that the information shall cover which rights may be restricted, the reasons and the potential duration. However, neither the █████, nor the █████ include any reference to such restrictions.
41. In view of the above, the EDPS **recommends** that █████ ensure compliance of the possible data transmission with the requirements of the EUDPR and their own internal rules on restrictions of certain rights of data subjects. More generally, even if the data transmission does not take place, █████ should amend its data protection records and its privacy statement on meetings and events in order to comply with the transparency requirements of Article 14 EUDPR.

3.3. Protocol No 7 on privileges and immunities

42. Protocol (No 7) on the privileges and immunities of the European Union²⁴ (‘Protocol No 7’) applies to █████ based on Article █████.

Inviolability of the archives of the Union, Article 2 of Protocol No 7

43. The protections afforded by Protocol No 7 extend to personal data contained in the archives of the EUIs insofar as such archives contain personal data²⁵. Indeed, the high level of protection that Article 8 of the Charter²⁶ and Article 16 TFEU²⁷ afford to personal data include, whenever applicable, the protection afforded by the Protocol insofar as inviolable archives of the Union contain personal data. In that sense, Article 8 of the Charter should be interpreted in conformity with the provisions on the secrecy of Union archives in Article 2 of the Protocol in order to protect against disclosure of personal data, which are part of such archives.

²² Article █████ of the rules on restrictions.

²³ Article █████ of the rules on restrictions.

²⁴ [Protocol \(No 7\) on the privileges and immunities of the European Union](#), OJ 2016/C 202, p. 266.

²⁵ See [EDPS Decision of 13 July 2023](#) on the Court of Justice of the EU’s request to authorise the contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. for transfers of personal data in the Court’s use of Cisco Webex and related services, §28.

²⁶ [Charter of Fundamental Rights of the European Union](#), OJ 2000/C 364/01.

²⁷ [Treaty on the Functioning of the European Union](#), OJ 2012/C 326/47.

44. The autonomous concept of ‘archives of the Union’ has been interpreted broadly by the Court of Justice²⁸. It covers any document “*of whatever date, of whatever type and in whatever medium which have originated in or been received by [EUIs] or by their representatives or servants in the performance of their duties, and which relate to the activities of or in the performance of the tasks of those entities.*”²⁹
45. The participants’ list held by █████ is thus possibly a document benefitting from protection under Article 2 of Protocol No 7.
46. The assessment of the compliance with the Protocol is however not required for the purposes of this Supervisory Opinion. Nevertheless, the EDPS **recommends** that the █████ consider the provisions of the Protocol.

4. CONCLUSION

47. As indicated above, in order to ensure compliance of the processing with the Regulation, the EDPS **deems necessary** that █████ ask the █████ to further substantiate the specific purpose of the transmission of the data at stake (list of participants to a specific event organised by █████), and why such transmission is necessary for the █████ to perform their tasks and proportionate to the goal pursued.
48. The EDPS also **recommends** that █████ further explore whether and how they could limit the amount of data communicated to the █████. They could for example ask that the █████ provide additional information as to the type of individuals/organisations they are targeting, so that █████ could remove from the list of participants the profiles that are not relevant for the █████.
49. In addition, the EDPS **recommends** that █████ ensure compliance of the possible data transmission with the requirements of the EUDPR and their own internal rules on restrictions. More generally, even if the data transmission does not take place, █████ should amend its record and privacy statement on meetings and events in order to comply with the transparency requirements of Article 14 EUDPR.

²⁸ [European Commission and ECB v. Republic of Slovenia](#), C-316/19, ECLI:EU:C:2020:1030, §§ 67-75.

²⁹ *Idem*, §75.

In light of the accountability principle, the EDPS expects [REDACTED] to implement the above recommendations accordingly and has decided to **close the case**.

Done at Brussels on 9 January 2024

(e-signed)

Wojciech Rafał WIEWIÓROWSKI