



EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION 3/2025

ON THE DRAFT DECISION OF THE MANAGEMENT BOARD OF THE EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY ADOPTING IMPLEMENTING RULES FOR THE APPLICATION OF REGULATION (EU) 2018/1725, INCLUDING RULES CONCERNING THE DATA PROTECTION OFFICER (Case 2025-0155)

1. INTRODUCTION

1. This Supervisory Opinion relates to the draft Decision of the Management Board of the European Insurance and Occupational Pensions Authority ('EIOPA') adopting implementing rules for the application of Regulation (EU) 2018/1725¹ ('the Regulation'), including rules concerning the Data Protection Officer ('DPO') pursuant to Article 45(3) of the Regulation ('draft decision').
2. EIOPA submitted the request for consultation to the European Data Protection Supervisor ('EDPS') on 5 February 2025.
3. The EDPS issues this Supervisory Opinion in accordance with Articles 41(1) and 57 (1)(g) of the Regulation.

¹ 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. LEGAL ANALYSIS AND RECOMMENDATIONS

2.1. General comments

4. The EDPS welcomes the adoption of the draft decision on implementing rules concerning data protection at EIOPA and its DPO.
5. The EDPS considers that the DPO is fundamental in ensuring the respect of data protection principles within EUIs².
6. The EDPS takes note that Article 3(1) of the draft decision provides that the Executive Director of the EIOPA shall appoint the DPO from amongst the staff of EIOPA on the basis of his/her expert knowledge of data protection law and practices as well as his/her sound knowledge of EIOPA's mandate, its structure, its administrative rules and procedures. **The EDPS welcomes this approach³**: in order to ensure proper knowledge of the functioning of EIOPA, the DPO should as a general rule be a staff member, in line with the first sentence of Article 43(4) of the Regulation.
7. Without prejudice to the application of all the principles and rules set out by the Regulation, **the EDPS issues the following recommendations to address additional details** that should be implemented to achieve higher level of protection.

2.2. EDPS recommendations

8. Article 2 of the draft decision provides the definitions for the purposes of the decision. Article 6(2) of the draft decision provides that the DPO may be assisted in his/her day-to-day activities by a DPO-assistant. Article 6(3) of the draft decision provides that the DPO may delegate his/her tasks and be represented (in his/her absence or when otherwise engaged) by one or more deputies, as necessary. The EDPS welcomes this approach since according to the size of the EUI and the nature of the processing operations that they carry out, it might be necessary for the DPO to have assisting staff⁴. However, the EDPS notes that Article 2 of the draft decision does not provide the definitions of 'DPO-assistant' and 'Deputy DPO'. Therefore, **the EDPS recommends that EIOPA include the definitions of 'DPO-assistant' and 'Deputy DPO' in Article 2 of the draft decision indicating that the DPO-**

² Point 2 of the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies.

³ Point 3.3 of the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies.

⁴ Ibidem.

assistant will support the DPO in his/her day-to-day activities, and that the Deputy DPO will support the DPO in his/her tasks and duties, and will deputise in the event of the DPO's absence or when otherwise engaged (Recommendation No. 1).

9. Article 4(4)(a) of the draft decision provides that one of the DPO's tasks is to inform/advise on the application of the provisions laid down in the Regulation, including with regard to the drafting of Data Protection Impact Assessments (DPIAs). The EDPS notes that it is the responsibility of the data controllers, not of the DPO, to carry out DPIAs⁵. In this context, the DPO can play an important role in advising EIOPA on whether to carry out a DPIA. The DPO can also advise on different aspects, for example, the type of methodology to use, or the technical and organisational security measures that EIOPA could apply to mitigate any risks to the rights and freedoms of the data subjects. Additionally, the DPO can provide guidance on the correct performance of the DPIAs, and on whether its conclusions comply with the Regulation. Therefore, **the EDPS recommends that EIOPA include another DPO task in Article 4(4) of the draft decision** indicating that the DPO shall:
 - advise on the **correct implementation of the DPIA** for a particular processing operation;
 - advise on what **methodology** to use on a case-by-case scenario;
 - provide support to the responsible staff to **analyse what are the data protection risks** of the processing operations under their responsibility; and,
 - advise on the selection of the necessary **safeguards to mitigate the risks** to the rights and freedoms of data subjects (**Recommendation No. 2**).
10. Article 5(1)(b) of the draft decision provides that the DPO may investigate issues and facts (on his/her own initiative or at the request of the Executive Director or the internal controllers, EIOPA's Staff Committee or any individual) which relate directly to his/her powers and responsibilities, and which have been brought to his/her knowledge. He/she shall consider them in accordance with the principle of impartiality and with due regard to the rights of the data subject. The EDPS underlines the importance of this DPO power when monitoring compliance with the Regulation. However, the EDPS notes that Article 5(1)(b) of the draft decision does

⁵ Point 5.2 EDPS Position Paper on the role of the DPOs of EUIs.

not include some relevant requirements in relation to the investigation procedure⁶. Therefore, **the EDPS recommends that EIOPA add a specific Article in the draft decision to describe the investigation procedure and clarify that the DPO shall:**

- send an **acknowledgment of receipt** to the person who commissioned the investigation and verify whether the request is to be treated as confidential.

- in the event of manifest abuse of the right to request an investigation, **inform the applicant that the request is not being pursued and give account of the reasons**. It is important to ensure that the applicant is well informed by the DPO of the underlining reasons why the request would not be pursued, for example where the request is repetitive, abusive and/or pointless.

- request a **written statement on the matter from the responsible staff** for the data processing activity in question, as well as complementary information (**Recommendation No. 3**).

11. Article 5(1)(e) of the draft decision provides that the DPO may bring to the attention of the Executive Director and the Human Resources Unit any failure by a staff member to comply with the obligations pursuant to the Regulation. The EDPS highlights the importance of informing the staff member and their manager in advance before reporting any failure to comply with data protection rules⁷. Therefore, **the EDPS recommends that EIOPA update Article 5(1)(e) of the draft decision by clarifying that the Executive Director and the Human Resources Unit may be notified after the DPO has informed the concerned staff members and their managers and suggested safeguards to prevent similar future incidents (Recommendation No. 4).**
12. Article 6(1) of the draft decision provides that EIOPA shall provide the DPO with the necessary resources to carry out his/her tasks and duties. The EDPS welcomes the wording that EIOPA shall support the DPO in performing his/her tasks by providing resources necessary to carry out those tasks⁸. The EDPS notes that this implies that the DPO should be provided not only with adequate support in terms of financial

⁶ As an example, you may see Article 12 of the EDPS Decision of 11 December 2018 on the implementing rules concerning the Data Protection Officer.

⁷ As an example, you may see Article 5.1.c of the EDPS Decision of 11 December 2018 on the implementing rules concerning the Data Protection Officer.

⁸ Article 44.2 of the Regulation.

resources, infrastructure (premises, facilities, equipment) and staff where appropriate, but also that the senior management actively supports the DPO function⁹. Therefore, **the EDPS recommends that EIOPA include another obligation in Article 6 of the draft decision indicating that the designation of the DPO shall be communicated officially to all staff.** This official communication to all staff will ensure that everyone knows about the DPO function within EIOPA. And this will facilitate that senior management and other services, such as the legal service or the communication team, can provide the DPO of EIOPA with the necessary active support (**Recommendation No. 5**).

13. Article 7 of the draft decision provides for the rules applicable to the cooperation with the DPO. The EDPS observes that the DPO shall foster a high level of data protection compliance in the organisation by cooperating with EIOPA staff responsible for procedures, training and advice on data processing and fundamental rights protection. Indeed, the EDPS notes that the DPO plays an important role in developing knowledge on data protection issues inside EIOPA. The EDPS highlights the positive consequences in terms of stimulating an efficient preventive approach rather than repressive data protection supervision. Therefore, **the EDPS recommends completing Article 7 of the draft decision by including a requirement that the DPO should also raise awareness and provide advice to the staff on practical recommendations for improvement of data protection within EIOPA, or concerning the interpretation or application of the Regulation¹⁰. (Recommendation No. 6).**
14. Article 7(1) of the draft decision provides the DPO shall be consulted, as appropriate, with regard to internal projects directly relating to the application of the provisions of the Regulation, and shall be informed about other legal acts related to EIOPA's mandate providing for the processing of personal data. The EDPS observes that this Article of the draft decision does not refer to the need for the DPO to take into account the guidelines issued by the EDPS. Since the data protection implications of some functions that are common to all EUIs are similar, the EDPS publishes regularly guidelines on specific subjects. The EDPS consolidates his guidance from previous supervisory opinions and consultations and include relevant guidance issued by the European Data Protection Board ('EDPB') and the Article 29 Working Party, as well as the case law of the European courts. Therefore, **the EDPS recommends that EIOPA complete Article 7(1) of the draft decision by indicating that the DPO**

⁹ Point 4.2 of the EDPS Position Paper on the role of DPOs of EUIs.

¹⁰ Point 6.1 of the EDPS Position Paper on the role of DPOs of EUIs.

shall take into account opinions and position papers of the EDPS directly relating to the internal application of the provisions of the Regulation. The inclusion of this requirement in the draft decision will ensure that the DPO of EIOPA will take into account the guidelines issued by the EDPS in the different fields when performing his or her duties **(Recommendation No. 7).**

15. Article 9 of the draft decision provides for the rules applicable to joint controllers. Pursuant to the Regulation, there is a need to conclude formal arrangements with joint controllers¹¹ to allocate responsibilities for compliance with the Regulation. Therefore, **the EDPS recommends that EIOPA include an obligation in the draft decision indicating that responsible staff members shall consult the DPO on those draft agreements (Recommendation No. 8).**
16. Article 10(2)(c) of the draft decision provides that the DPCs and/or staff member processing personal shall assist the (internal) controller and the DPO in the assessment of risks certain processing activities pose to the fundamental rights and freedoms of data subjects and document it in a record. According to Article 45(1)(e) of the Regulation, the DPO shall *provide advice where requested* (our emphasis) as regards the DPIA and monitor its performance pursuant to Article 39 and to consult the EDPS in case of doubt as to the need for a DPIA. As noted above (point 10), the EDPS observes that it is the responsibility of the data controllers, not of the DPO, to carry out DPIAs¹². Therefore, **the EDPS recommends to update article 10(2)(c) of the draft decision clarifying that the DPCs and/or staff member processing personal data shall assist the (internal) data controller in the assessment of risks that certain processing activities pose to the fundamental rights and freedoms of data subjects and document it in a record, and they may request the DPO to provide advice on the correct implementation of the DPIA (Recommendation No. 9).**
17. Article 13 of the draft decision provides that when data subjects contact EIOPA to exercise their rights pursuant to Articles 17 to 24 of Regulation, the relevant EIOPA staff members and/or the DPCs shall assist the DPO and the (internal) data controller in replying to the data subject's request. Pursuant to the Regulation¹³, the controller shall facilitate the exercise of data subject rights. The EDPS observes that EIOPA, which bears the legal responsibility for ensuring compliance with the Regulation, shall ensure that the data subject can exercise their rights and ensures

¹¹ Article 28 of the Regulation.

¹² Point 5.2 EDPS Position Paper on the role of the DPOs of EUIs.

¹³ Article 14(2) of the Regulation.

respect of the principles established in the Regulation¹⁴. Therefore, **the EDPS recommends that EIOPA update Article 13 of the draft decision by clarifying that the EIOPA responsible staff members (DPCs or internal data controllers) shall consult the DPO before acting in reply to the data subject's request¹⁵. In addition, the EDPS recommends that EIOPA clarify that in case the DPO acts as responsible staff for managing data subjects' requests on behalf of the data controller, it shall be detailed in an operational manual (Recommendation No. 10).**

3. CONCLUSION

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

Brussels, 3 March 2025

(e-signed)

Wojciech Rafał WIEWIÓROWSKI

¹⁴ Section 2 of the EDPS Position Paper on the role of DPOs of EUIs.

¹⁵ As an example, you may see Article 13 of the EDPS Decision of 11 December 2018 on the implementing rules concerning the Data Protection Officer.