



EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION ON THE DRAFT DECISION ESTABLISHING MEASURES FOR THE APPLICATION OF REGULATION (EU) 2018/1725, INCLUDING MEASURES CONCERNING THE DATA PROTECTION OFFICER OF THE EUROPEAN UNION DRUGS AGENCY (Case 2024-0819)

1. INTRODUCTION

1. This Supervisory Opinion relates to the draft Decision of the Management Board of the European Union Drugs Agency ('EUDA') establishing measures for the application of Regulation (EU) 2018/1725¹ ('the Regulation'), including measures concerning the Data Protection Officer ('DPO') pursuant to Article 45(3) of the Regulation ('draft decision').
2. EUDA submitted the request for consultation to the European Data Protection Supervisor ('EDPS') on 18 September 2024.
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 EUDA 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 EUDA appoints the DPO from amongst EUDA staff on the basis of his/her personal and professional qualities and in particular, his or her expert knowledge of data protection. **The EDPS welcomes this approach**³: in order to ensure proper knowledge of the functioning of the EUDA, 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. The draft decision provides a definition of ‘controller’: Article 2(a) of the draft decision provides that the controller shall mean the Executive Director or the Head of the Unit to whom the Executive Director may delegate her/his tasks. According to Article 3(8) of the Regulation, controller means the Union institution or body or the directorate-general or any other organisational entity which alone or jointly with others, determines the means and the purposes of the processing of personal data. The EDPS understands the need to designate the Executive Director of the EUDA or the Head of the Unit to whom the Executive Director may delegate her/his tasks as the controller. However, the EDPS notes that although a person (i.e., Director or Head of Unit) is de facto responsible for the processing operation, they, as officials, are acting on behalf of the EUDA, which bears the legal responsibility for ensuring compliance with the Regulation⁴. Therefore, **the EDPS recommends that the**

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

EUDA clarify the terminology by designating the EUDA as the Data Controller, represented by its Executive Director who may delegate her/his tasks to the Head of the Units to reflect operational responsibilities, in order to reflect who bears the legal responsibility for ensuring compliance with the Regulation, in line with Article 3(8) of the Regulation (Recommendation No.1). In addition, the EDPS recommends that the EUDA should not use the expression controllers in the plural, since the expression of ‘controller’ is in singular according to the definition provided in Article 3(8) of the Regulation (Recommendation No.2).

9. Article 3(6) of the draft decision provides that the DPO shall be provided with adequate resources necessary to carry out his or her duties. The EDPS welcomes the wording that the EUDA shall support the DPO in performing his/her tasks by providing resources necessary to carry out those tasks⁵. The EDPS notes that this implies that the DPO should be provided not only with adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate, but also that the senior management actively supports the DPO function⁶. **The EDPS recommends that the EUDA include an obligation in Article 3(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 the EUDA. And this will facilitate that senior management and other services, such as the legal service or the communication team, can provide the DPO of the EUDA with the necessary active support **(Recommendation No.3).**
10. The EDPS observes that Article 3 of the draft decision does not include some relevant requirements in relation to the status/position of the DPO. According to Article 44(2) of the Regulation, the Union institutions and bodies shall support the DPO by providing resources necessary to maintain his or her expert knowledge. The EDPS emphasises the need to provide the DPO with continuous training and to be given the opportunity to stay up to date with regard to developments within the field of data protection⁷. Therefore, the **EDPS recommends that the EUDA update Article 3 of the draft decision by including a requirement that the DPO shall have access to the necessary training and the opportunity to maintain his or her knowledge up-to-date with regard to the legal and technical aspects of data protection,** in line with Article 44(2) of the Regulation. The aim should be to constantly increase the level of expertise of the DPO and he/she should be encouraged to participate in training courses on data protection, meetings of the

⁵ Article 44.2 of the Regulation.

⁶ Point 4.2 of the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies.

⁷ Ibidem.

DPO network, and other forms of professional development, such as participation in privacy fora and workshops⁸ (**Recommendation No.4**).

11. Article 4(4) of the draft decision provides that the DPO shall keep a central register of the processing operations carried out by the controllers and grant access to such register to any person directly or indirectly through the EDPS. Article 31 of the Regulation provides that it is the responsibility *of the controller* (our emphasis) to maintain the records of processing activities relating to specific processing operations. In addition, according to Article 31(4) of the Regulation, the Union institutions and bodies shall make the record available to the EDPS on request. Moreover, Article 31(5) of the Regulation establishes that Union institutions and bodies shall keep their records of processing activities in a central register and they shall make the register publicly accessible. Therefore, **the EDPS recommends that the EUDA revise Article 4(4) of the draft decision by deleting the references to ‘the DPO keeping a central register of the processing operations carried out by the controllers and grant access to such register to any person directly or indirectly through the EDPS’**. Firstly, to require the DPO to keep a central register of the processing operations would be against to what is legally established in Article 31 of the Regulation. Indeed, it is the data controller, not the DPO, who is required to maintain a record of processing operations under its responsibility. And secondly, the referred ‘indirect access through the EDPS’ is also not included in any of the legal provisions of the Regulation (**Recommendation No. 5**).
12. Article 4(5) of the draft decision provides that the DPO shall notify the EDPS of the processing operations likely to present risks referred to in Article 39(1) of the Regulation. According to Article 45(1)(e) of the Regulation, the DPO shall provide *advice where requested* (our emphasis) as regards the data protection impact assessment (‘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. Indeed, the DPO can play an important role in advising EUDA 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 measures that EUDA 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 the EUDA update Article 4(5) of the draft decision clarifying that the controller may request the DPO to provide advice on the correct implementation of the DPIA in relation to processing operations likely to present a high risk referred to in Article 39(1) of the Regulation, monitor its**

⁸ Ibidem.

performance and consult the EDPS in case of doubt as to the need for a DPIA; and, in particular, clarifying that the DPO shall:

- provide support to responsible staff to assess the data protection risks relating to the processing activities under their responsibility;
- advise staff members on what methodology to use on a case-by-case basis; and,
- advise on the selection of necessary safeguards to mitigate the risks to the rights and freedoms of data subjects (**Recommendation No.6**).

13. Article 5 of the draft decision provides for the DPO's duties. 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. **The EDPS recommends completing Article 5 of the draft decision by indicating that the DPO shall be informed, as appropriate, about opinions and position papers of the EDPS directly relating to the internal application of the provisions of the Regulation, as well as about opinions concerning the interpretation or implementation of other legal acts related to the protection of personal data and access to personal data.** The inclusion of this requirement in the draft decision will ensure that the DPO of the EUDA will take account the guidelines issued by the EDPS in the different fields when performing his or her duties. (**Recommendation No.7**).
14. Article 5(1)(b) of the draft decision provides that the DPO shall on his/her own initiative or the initiative of the Executive Director, the controllers, the Staff Committee or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his/her notice, and report back to the Executive Director or the person who commissioned the investigation. **The EDPS welcomes this approach and recommends that the EUDA complete Article 5(1)(b) of the draft decision by indicating that the Staff Committee and all services of the EUDA must cooperate closely with the DPO in cases of an alleged breach of data protection rules, and ensure that they are duly informed and consulted⁹.** Indeed, it is important that the DPO receives the necessary and valuable support and

⁹ Point 5.5 of the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies.

close cooperation from the Staff Committee and all services of the EUDA when monitoring compliance with the Regulation. **(Recommendation No.8).**

15. Article 7(2)(b) of the draft decision provides that the controller shall assist the DPO and the EDPS in performing their respective duties, in particular by giving information in reply to their requests within thirty days. The EDPS notes that there may be situations in which the controller should provide the DPO with all the necessary information in a shorter period of time to enable him/her to perform his/her respective duties. For example, in the context of an investigation procedure, the controller shall provide his/her response to the DPO within five working days. Therefore, **the EDPS recommends that the EUDA update Article 7(2)(b) of the draft decision by indicating that the controller shall provide the information in reply to the requests of the DPO and the EDPS within a reasonable period, depending on the circumstances of the case, and in any case, no later than thirty days.** Indeed, the receipt of the information in a reasonable period will allow the DPO to carry out its duties properly **(Recommendation No.9).**

16. Article 9(2) of the draft decision provides that the information entered in the central register by the DPO may exceptionally be limited when it is necessary to safeguard the security of a specific processing operation. According to Article 31(1) of the Regulation, each controller shall maintain a record of processing activities under its responsibility. The record required under Article 31 of the Regulation consists in a tool allowing the data controller and the EDPS, upon request, to have an overview of all the personal data processing activities carried out. It is thus a prerequisite for compliance, and as such, an effective accountability measure¹⁰. More detailed records of processing activities can be kept internally by the controller, however, the records of processing activities which are published in the publicly accessible register must, at a minimum, contain the information listed in Article 31(1) of the Regulation. Moreover, in line with Article 31(1)(g) of the Regulation, the record of processing activities shall where possible, contain a general description of the technical and organisational security measures referred to in Article 33 of the Regulation. Indeed, the publicly available record shall contain only a general description on the security measures in place, but a more detailed description of the measures should be kept internally by the EUI. Therefore, **the EDPS recommends that the EUDA delete the second sentence of Article 9(2) of the draft decision referring to ‘the information entered in the central register by the DPO may exceptionally be limited when it is necessary to safeguard the security of a specific processing operation’** to clarify that all records of processing activities under the responsibility

¹⁰ Point 5.3 of the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies.

of the controller shall contain, at a minimum, all the information listed under Article 31(1) of the Regulation (**Recommendation No.10**).

17. Article 11 of the draft decision provides for the rules applicable to the investigation procedure. In particular, Article 11(2) of the draft decision provides that the DPO shall send acknowledgment of receipt to the requester within five working days. **The EDPS welcomes this approach and recommends that the EUDA complete Article 11(2) of the draft decision clarifying that in the event of manifest abuse of the right to request an investigation, the DPO shall inform the applicant that the request is not being pursued and give account of the reasons¹¹.** 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 (**Recommendation No.11**).
18. The EDPS observes that the draft decision does not include provisions on the handling and communication of personal data breaches¹². Pursuant to the Regulation, the controller shall inform the DPO about personal data breaches¹³. Additionally, where requested, the DPO provides advice as regards the necessity for a notification to the EDPS or a communication of a personal data breach to the affected data subjects¹⁴. The responsible staff members (including the local information security officer, depending on the EUDA's internal procedures) need to inform the DPO without undue delay, including when they have doubts on whether personal data are affected by the security breach. **Therefore, the EDPS recommends that the EUDA establish and describe a procedure¹⁵ for the handling and notification of data breaches involving the DPO as well as the security officer (or the staff member having a similar role).** Indeed, the DPO shall be provided with all the necessary information enabling him/her to ensure that the EUI comply with the Regulation and more specifically with the obligations on personal data breach notifications and communications in accordance with Articles 34 and 35 of the Regulation (**Recommendation No 12**).

¹¹ 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.

¹² Article 34 and 35 of the Regulation.

¹³ Article 34.5 of the Regulation.

¹⁴ Points 4.1 and 5.2 of the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies.

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

3. CONCLUSION

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

Done at Brussels