EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

18 December 2025

Supervisory Guidance

Role of the Data Protection Officers in EU institutions, bodies, offices and agencies

edps.europa.eu

Executive Summary

This Supervisory Guidance sets out the European Data Protection Supervisor's (EDPS) interpretation of the role, position, and tasks of Data Protection Officers (DPOs) in Union institutions, bodies, offices and agencies (EUIs) under Regulation (EU) 2018/1725 (EUDPR).

It provides practical and updated guidance on the designation of DPOs, their position within EUIs, the guarantees of independence attached to the function, and the tasks entrusted to them. The Guidance builds on the EDPS Position Paper of 2018, experience acquired since the entry into force of the EUDPR, the results of the 2023 EDPS survey on the position of DPOs, and exchanges within the DPO network.

The Guidance aims to support EUIs in ensuring the effective, independent, and consistent application of Union data protection law, while reinforcing the DPO's role as a key internal safeguard for the protection of personal data.

Contents

1. Introduction

1. The protection of natural persons in relation to the processing of their personal data is a fundamental right laid down in Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter'),[1] Article 16(1) of the Treaty on the Functioning of the EU ('TFEU')[2] and Article 8 of the European Convention on Human Rights.[3] Data protection is closely linked to the right to respect for private and family life protected by Article 7 of the Charter.[4]

2. Following the adoption of the General Data Protection Regulation ('GDPR'),[5] Regulation (EU) 2018/1725 (the 'EUDPR') aligned the data protection rules for Union institutions, bodies, offices and agencies (EUIs) with the GDPR rules to provide a strong and coherent data protection framework across the European Union.

3. The EUDPR lays down rules on the protection of natural persons with regard to the processing of personal data by EUIs and the free movement of such data. It protects fundamental rights and freedoms of natural persons and particularly their right to the protection of personal data. The EUDPR applies to the processing of personal data by all EUIs when the processing is carried out in the exercise of activities, which fall, wholly or partially, within the scope of Union law.[6]

4. The data controller, defined in the EUDPR as 'the Union institution, body, office or agency or the Directorate-General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data',[7] is responsible for, and should be able to demonstrate compliance with the EUDPR (principle of accountability).[8] The data controller often has insight into the processing operation itself. The data controller should therefore ensure that the data subject can exercise their rights and ensures respect of the principles established in the EUDPR. It should be noted that although a person (e.g. Head of Unit or Director) or an organisational part of the institution (e.g. the HR Unit or the Security Unit) or body is *de facto* responsible for the processing operation,

---

[1] Article 8 Protection of personal data:
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[2] Article 16 TFEU:
1. Everyone has the right to the protection of personal data concerning them. (...)

[3] Article 8 Right to respect for private and family life:
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[4] Article 7 Respect for private and family life:
Everyone has the right to respect for his or her private and family life, home and communications.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 119, 4.5.2016, p. 1–88).

[6] Article 2(1) EUDPR.

[7] Article 3(8) EUDPR.

[8] Articles 4 and 26(1) EUDPR.

they, as officials, are acting on behalf of the EUI, which bears the legal responsibility for ensuring compliance with the EUDPR.

5. The EUDPR provides the obligation for each EUI to designate a DPO.[9] The DPO is fundamental in ensuring the respect of data protection principles within EUIs.

6. The Founding Regulations of the European Union Agency for Law Enforcement Cooperation (Europol),[10] the European Union Agency for Criminal Justice Cooperation (Eurojust),[11] and the European Prosecutor's Office (EPPO)[12] also include provisions on the DPO, which generally replicate the EUDPR but also contain specific rules.[13]

7. The EUDPR provides for an independent supervisory authority, the EDPS, responsible for monitoring the processing of personal data by EUIs.[14] This supervisory role includes providing support, within the institutional framework, to the work and function of DPOs.

8. DPOs have existed within EUIs since 2002 and have demonstrated their value not only through their internal role, but also through the establishment of a DPO network. This network, which meets regularly, including with the EDPS, has facilitated the exchange of views on common issues and challenges.

9. This Supervisory Guidance intends to provide updated guidance for DPOs in their role, building on the principles and recommendations contained in the previous 2018 EDPS Position Paper on the role of DPOs of EUIs as well as on the experience acquired since the entry into force of the EUDPR and other legal instruments regulating the processing of personal data in the area of freedom, security and justice. This Guidance also draws from the EDPS Survey on the designation and position of the data protection officer in the EU institutions, bodies, offices and agencies,[15] as well as insights from workshops held during the EDPS-DPOs meetings of 30 November 2023 and 2 July 2025. It also takes account of the contributions provided to the EDPS by the DPO network.

Examples or recommended practices appear in a box within the text.

---

[9] Article 43(1) EUDPR.

[10] 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 (the '**Europol Regulation**'), OJ L 135, 24.5.2016, pp. 53–114 (Consolidated version -28/06/2022). See Articles 41, 41a and 41b of the Europol Regulation.

[11] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (the '**Eurojust Regulation**'), OJ, L 295, 21.11.2018, p. 138 (Consolidated version - 31/10/2023). See Articles 36-38 of the Eurojust Regulation.

[12] Council Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (the EPPO) (the '**EPPO Regulation**'), OJ, L283, 31.10.2017, p. 1 (Consolidated version - 10/01/2021). See Articles 77-79 of the EPPO Regulation.

[13] This Guidance will refer to these specific rules in footnotes where necessary. See *Annex - Provisions on the DPO - Cross-reference table*.

[14] Articles 1(3), 52 EUDPR.

[15] Launched in March 2023, the survey was part of the 2023 European Data Protection Board's (EDPB) Coordinated Enforcement Action that the EDPS conducted alongside the other 26 data protection authorities of the European Union (EU) and the European Economic Area (EEA), on the role, responsibilities and tasks of DPOs. The survey report was published on 18 January 2024. See EDPS press release.

2. Designation of the DPO

2.1. Mandatory designation of a DPO (Article 43(1) EUDPR)

10. The EUDPR requires that each EUI must designate a DPO.[16]

11. EUIs are 'Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU, the TFEU or the Euratom Treaty'.[17] The designation of the DPO should be formalised through an internal decision adopted at the highest management level of the EUI.[18] Decisions on reappointment should follow the same formal procedure.

12. The DPO must be appointed for a mandatory minimum term[19] and their designation must be notified to the EDPS.[20]

13. The appointment or reappointment of the DPO should be transparently communicated within the EUI, for example via the intranet or via other appropriate internal channels.[21]

2.2. Designation of a single DPO for several EUIs (Article 43(2) EUDPR)

14. The EUDPR provides for the possibility for EUIs to designate a single DPO for several of them, taking into account their organisational structure and size.[22]

15. Where the appointment of a single DPO for several EUIs ('shared DPO') is envisaged, the EUIs concerned must carefully assess the feasibility of such an arrangement, considering, in particular, their respective size, mandate and geographical location, as well as the volume and sensitivity of the personal data that they both process.

16. The terms governing cooperation between the EUIs concerned with regard to the shared DPO should be clearly laid down in writing. All provisions of the EUDPR apply fully to each EUI, notwithstanding the shared nature of the DPO function. Particular attention should therefore be paid to the rules on conflict of interests,[23] the term of designation,[24] and the provision of necessary resources.[25] It remains the responsibility of the designating EUIs to ensure that the arrangement functions effectively in practice and that the shared DPO is able to carry out their DPO tasks satisfactorily for all EUIs concerned.

---

16 Article 43(1) EUDPR.
17 Article 3(10) EUDPR. A list of EUIs is available on the EDPS website.
18 On the 'highest management level', see section 3.3.3. *Direct reporting to the highest management level* (Article 44(3), third sentence EUDPR).
19 See section 3.5. *Term of designation* (Article 44(8), first sentence, EUDPR).
20 See section 3.7. *Registration with the EDPS* (Article 44(9) EUDPR).
21 See section 2.5. *Publication of contact details* (Article 43(5) EUDPR).
22 Article 43(2) EUDPR.
23 Article 44(6) EUDPR. See section 3.4. *No conflict of interests* (Article 44(6) EUDPR).
24 See section 3.5. *Term of designation* (Article 44(8), first sentence, EUDPR).
25 See section 3.2. *Necessary resources* (Article 44(2) EUDPR).

17. First, EUIs must consider the risk of conflicts of interests, particularly in relation to transmissions of personal data between the EUIs concerned. In such situations, the DPO may be required to advise on the necessity of the transmission. Where this creates a conflict, alternative arrangements must be put in place.

> *If a shared DPO is asked to provide advice on the necessity of data transmissions between their two EUIs, the assistant DPO or another staff member appointed to this end could be in charge of the assessment of the transmission. Alternatively, the opinion of the DPO of another EUI could be sought. Depending on the case and the available alternatives, the EDPS could also be consulted.*

18. Second, given that the DPO must be designated for a term of three to five years, EUIs appointing a shared DPO must ensure that the respective mandates are compatible with one another and comply with Article 44(8) EUDPR. This is particularly relevant where the existence of one mandate is a precondition for the other.

> *Official A is a staff member of EUI X. Their mandate as DPO of EUI X ends on 31 August 2026. A is also appointed as DPO of EUI Y with effect from 1 January 2026 for a three-year term. Consequently, their mandate as DPO of EUI X would expire before the end of their mandate for EUI Y, with the result that their designation as DPO of EUI Y would not meet the required minimum duration of three years.*
> *By contrast, if A's term as DPO of EUI X ends on 31 December 2029, they may be appointed as DPO of EUI Y from 1 January 2026 for a full three-year term.*

19. Thirdly, each EUIs must ensure that the shared DPO is provided with the necessary resources and training to carry out their duties.

20. Fourthly, the shared DPO, supported where appropriate by a team, must be able to communicate effectively with controllers, staff members and data subjects.

> *Availability is essential to ensure that data subjects can contact the DPO. A minimum level of physical presence should be ensured in order to build trust with controllers and staff and to enable the DPO to gain a thorough understanding of the EUI's activities. Even occasional physical presence can enhance the quality and effectiveness of the advice provided.*

21. In summary, the appointment of a shared DPO should remain exceptional and should be duly justified.

> *As a matter of good practice, EUIs are encouraged to seek the EDPS' supervisory opinion before deciding to appoint a shared DPO.*

2.3. Expertise and skills of the DPO (Article 43(3) EUDPR)

22. The DPO shall be designated on the basis of professional qualities, in particular, expert knowledge of data protection law and practices, and the abilities to fulfil their tasks.[26] Two aspects are particularly important: a sound understanding of the organisation, structure and functioning of the EUI, and robust expertise in data protection. This expertise should include knowledge of risk management and analysis, information technology and algorithmic systems.

23. The required level of expertise is not further defined in the EUDPR, but it must correspond to the size of the EUI and the sensitivity, complexity and amount of personal data that they process.[27]

24. Where the required expertise is not available inside the organisation, EUIs may need to launch an external selection procedure.

25. Providing the DPO with adequate resources includes continuous training. This can be ensured both at the time of entry into function and by regular up-dates during the mandate.[28]

26. Ability to fulfil the tasks incumbent on the DPO should be interpreted as referring to both their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include organisational and communication skills, as well as integrity and high professional ethics.

27. To ensure a consistent and informed approach to data protection compliance, the EDPS recommends that staff supporting the DPO, and Data Protection Coordinators (DPCs)[29] also have a thorough understanding of the EUDPR and other relevant data protection rules.

2.4. Internal or external DPO (Article 43(4) EUDPR)

28. The EUDPR provides that the DPO shall be a staff member of the EUI.[30] The EUDPR allows the DPO function to be performed under on a service contract where certain conditions are met: Taking into account their size, and where the option of appointing a shared data protection officer is not exercised, EUIs may designate a data protection officer to perform their tasks under a service contract.[31]

29. Therefore, as a general rule, the data protection officer must be appointed from among the staff of the EUI.[32]

---

[26] Article 43(3) EUDPR.

[27] See recital 62 EUDPR: "That officer should be a person with expert knowledge of data protection law and practices, which should be determined in particular according to the data processing operations carried out by the controller or the processor and the protection required for the personal data involved."

[28] See section 3.2.4. *Training*.

[29] See section 3.2.3. *Human resources.*

[30] Article 43(4), first sentence EUDPR.

[31] Article 43(4), second sentence EUDPR. The possibility to designate an external DPO does not apply to the DPOs of Europol, Eurojust and EPPO, who must be staff members (Article 41(1) of the Europol Regulation, Article 36(1) of the Eurojust Regulation and Article 77(1) of the EPPO Regulation).

[32] According to the EDPS survey report on the position of the DPO (18 Jan 2024), all 69 respondents - covering 71 EUIs - were EUI staff members.

30. Designation of a DPO on the basis of a service contract should be considered only as a secondary option, in particular only where the size or structure of the EUI makes an internal appointment impracticable and where other organisational options are not used. Where an external DPO is designated, the EUI should be able to justify why an internal staff appointment was not appropriate in the specific circumstances.

31. Such externalisation of the DPO function is limited to an individual DPO and may not be entrusted to a legal entity.[33]

32. Several factors must be carefully assessed before externalising the DPO function.

33. First, the DPO function requires a high level of confidentiality which must also be fully ensured where the function is entrusted to an external contractor, and may be more difficult to guarantee in such arrangements.

34. Second, having in-depth knowledge of the functioning of the EUI - its mandate and functions, its management and staff, and its processing operations - is important to allow the DPO to carry out their functions effectively. Physical or organisational distance may hinder the provision of timely, well-informed and effective advice.

2.5. Publication of contact details (Article 43(5) EUDPR)

35. EUIs must publish the contact details of the DPO and communicate them to the EDPS.[34]

36. While the EUDPR does not require the publication of the DPO's name on the EUI's website, the DPO's contact details must be made available.

37. In addition, the DPO's contact details must be included in the information provided to data subjects both when their personal data are collected and where personal data have not been obtained from the data subject.[35]

> *As a practical measure, the EDPS recommends setting up a functional DPO mailbox, to be indicated in data protection notices, on the website, and in other public communications.*

38. Internally, staff members should be informed of the name and contact details of the DPO. This should be ensured through publication on the intranet, internal directories and organisational charts.

39. Communicating the name and contact details of the DPO to the EDPS is essential to enable the DPO to act as a contact point between the EUI and the EDPS.[36]

---

[33] See the wording of Article 43(4), second sentence EUDPR: '(...) a data protection officer **who** fulfils **his or her** tasks on the basis of a service contract'.

[34] Article 43(5) EUDPR.

[35] Articles 15(1)(b) and 16(1)(b) EUDPR.

[36] The EUDPR requires EUI to provide the contact details of their data protection officer in other limited but clearly defined set of situations: In particular, the DPO's contact details must be included in the information provided to data subjects when personal data are collected directly from them or obtained indirectly, both for administrative

2.6. Continuity of the DPO function

40. Since EUIs are required to designate a DPO, they must ensure the continuity of the DPO function at all times.

41. In certain cases, the DPO may no longer be able to fulfil their duties. This may apply to temporary circumstances, as well as prolonged absences (sick leave or leave on personal grounds), and departure from the EUI (resignation, retirement, or dismissal).

42. The EUDPR does not provide for the designation of a deputy or assistant DPO.[37] The EDPS nevertheless recommends that EUIs designate a deputy DPO to support and replace the DPO when they are unavailable. The designation of a deputy DPO should be notified to the EDPS.[38]

43. The deputy DPO should perform the tasks of the DPO during the latter's absence. Where no deputy DPO is designated, continuity of the DPO function requires the appointment of a temporary DPO.

44. EUIs should notify the EDPS of the designation of a temporary DPO and indicate the expected duration of the arrangement. In the event of a prolonged or permanent absence of the DPO, the EUI must designate a new DPO.

45. Any individual ensuring continuity of the DPO function must enjoy the same guarantees of independence as the designated DPO. They must perform their tasks independently, receive no instructions, and must not have conflicts of interests with other official duties.

3. Position of the DPO

3.1. Involvement of the DPO (Article 44(1) EUDPR)

46. The data controller must ensure that the DPO is involved, properly and in a timely manner, in all issues relating to data protection.[39]

47. This obligation reflects one of the aspects of building a data protection culture within the organisation. Early and systematic involvement of the DPO facilitates compliance with the EUDPR and promotes data protection by design and by default.[40] The DPO should therefore

---

and operational processing. They must also be communicated in the context of personal data breach management, namely in notifications to the EDPS and, where applicable, in communications to affected data subjects. In addition, processors acting on behalf of EUI are required to include the DPO's contact details in their records of processing activities. These obligations ensure that data subjects and supervisory authorities have a clear and accessible point of contact for all matters relating to data protection.

37 But see Article 41a(2), 2nd sentence of the Europol Regulation provides that 'In order to support the Data Protection Officer in carrying out his or her tasks, a member of staff of Europol may be designated as assistant Data Protection Officer'. According to Article 41a(10), 'The provisions applicable to the Data Protection Officer shall apply mutatis mutandis to the assistant Data Protection Officer.'

38 See section 3.7. *Registration with the EDPS* (Article 44(9) EUDPR).

39 Article 44(1) EUDPR.

40 Article 27 EUDPR.

be consulted whenever decisions with data protection implications are taken, irrespective of the hierarchical level at which they occur.

48. The DPO should be consulted during the planning phase of an information technology systems and other projects before they are launched. Early involvement allows potential issues to be identified and assessed at an early stage, such as whether personal data will be processed, which categories of data are involved, and the purposes of the processing.

> *As a good practice, EUI's may include a 'DPO consultation' checkbox in the EUI's project charter form or checkpoint in project planning or approval documentation.*

49. In addition, the DPO should be recognised as a key discussion partner within the EUI, and they should be involved in relevant working groups, steering committees, and other fora dealing with data processing activities. The EDPS also recommends that the DPO be invited to participate regularly in management meetings and that their opinions always be given due consideration.[41]

50. Timely involvement presupposes that the DPO is visible within the organisation and receives relevant information sufficiently early to provide meaningful advice.

51. The position of the DPO in the organisation chart is an important element of visibility. The DPO should be recognised as a distinct function within the organisation, with a clearly defined position in the organisation chart that reflects their direct reporting line to the highest management level.

52. The DPO visibility may be further enhanced through internal communications, such as newsletters, and through dedicated sections on the intranet and website.

53. The DPO should actively contribute to decision-making processes and maintain regular communication with senior management and the highest operational levels.[42] To facilitate this, the DPO should be regularly invited to top-level management meetings in order to report on data protection issues and remain informed about institutional developments. This regular interaction also ensures timely identification and resolution of data protection issues.

> *As a best practice, the DPO should be copied in all correspondence related to data protection matters involving the EDPS or other EUIs. The use of a functional DPO mailbox further supports business continuity.*

54. Article 44(1) EUDPR requires the controller to involve the DPO in *all* data protection-related issues.

55. In addition, the DPO may proactively provide advice to the controller as part of their duty to ensure the internal application of the EUDPR and to monitor compliance with the EUDPR (Article 45(1)(b) EUDPR).

---

[41] See section 3.3.3. *Direct reporting to the highest management level* (Article 44(3), third sentence EUDPR).
[42] See section 3.3.3. *Direct reporting to the highest management level* (Article 44(3), third sentence EUDPR).

56. In all circumstances, EUIs should give due consideration to the DPO's advice, whether solicited or provided proactively, as a key component of the controller's accountability obligations under Articles 4(2) and 26 EUDPR.

57. The controller may further define situations requiring consultation of the DPO, either in the implementing rules concerning the DPO adopted pursuant Article 45(3) EUDPR,[43] or in other relevant internal policies.

3.2. Necessary resources (Article 44(2) EUDPR)

58. The EUI shall support the DPO in performing their tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain their expert knowledge.[44]

59. Insufficient resources may compromise the DPO's ability to perform their duties effectively and may negatively affect the overall level of compliance within the EUI.

3.2.1. Material resources

60. The DPO should be provided with adequate support in terms of financial resources and infrastructure (premises, facilities, equipment). Moreover, the senior management should actively support the DPO function. Such support includes that the designation of the DPO is communicated officially to all staff to ensure that their existence and function are known within the EUI.[45]

3.2.2. Access to the personal data

61. Providing necessary resources also includes granting the DPO access to personal data, processing operations and premises insofar as this is required for the performance of their tasks. Such access enables the DPO to investigate issues directly related to their mandate.[46]

3.2.3. Human resources

62. DPOs should have sufficient time to fulfil their duties. They should also receive appropriate support from other services, such as legal, human resources or communication services.

63. The difference in size of the EUIs entails significant differences in resources. Larger EUIs have more staff to devote to DPO-related tasks and may even have a whole team supporting the DPO function, whereas smaller EUIs often only have part-time DPOs who carry out other tasks in parallel to their DPO tasks.[47]

---

[43] See section 5. *Implementing rules concerning the DPO*.
[44] Article 44(2) EUDPR.
[45] See section 2.5. *Publication of contact details* (Article 43(5) EUDPR).
[46] Article 45(2) EUDPR. See section 4.5. *Handling queries, complaints and other matters* (Articles 44(4) and (7) EUDPR and 45(2), second sentence, EUDPR).
[47] According to the EDPS survey report on the position of the DPO (18 Jan 2024), only 19 out of the all 69 respondents (covering 71 EUIs) were full-time DPOs.

A. Full-time and part-time DPOs

64. The EUDPR allows DPOs to fulfil other tasks and duties.[48] However, larger EUIs and those with significant data protection responsibilities, such as processing special categories of personal data as part of their core activities, or processing data relating to vulnerable data subjects should appoint a full-time DPO.

65. For part-time DPOs, the most important element is to have sufficient time to fulfil their duties. Otherwise, conflicting priorities could result in the DPO duties being neglected.

> *It is good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. For the calculation of this percentage, the working days, including travel time and preparation, for the DPO network meetings and the EDPS-DPOs meetings, should be taken into consideration.*

66. Determining the appropriate time allocation may be complex and is not solely dependent on the size of the EUI. Even small EUIs may engage in numerous or sensitive processing operations. In addition, newly created DPO functions or newly appointed DPOs typically require a significant initial investment of time to build awareness and establish compliance mechanisms.

67. The EDPS strongly recommends that EUIs consider appointing a full-time DPO, at least at the outset of the function. In any event, the EUI should not underestimate the workload associated with the DPO role when determining time allocation.

> *By way of illustration, assuming a baseline of 200 working days per year, an allocation of 10% for the DPO function corresponds to approximately 20 working days dedicated to data protection tasks annually. Given that participation in the two annual DPO network meetings may already require up to 4 days each (2 meeting days and 2 travel days), this would leave only around 12 days per year for the DPO to perform all remaining tasks under Articles 43–45 EUDPR.*

68. A way for the EUI to measure the time needed to carry out the function and to determine appropriate level of priority for DPO duties for part time DPOs, is to encourage DPOs to draw up a work plan that could be made available to hierarchy and staff. This work plan could also be a useful instrument in the evaluation of the DPO.

69. EUIs should periodically reassess the time allocated to the DPO function to ensure that it remains adequate.

---

[48] Article 44(6) EUDPR. By contrast, Article 41(1) of the Europol Regulation specifies that the DPO shall be designated 'for that sole position', thus expressly excluding the possibility to designate a part-time DPO for Europol.

B. DPO team

70. Depending on the size of the EUI and the nature of the processing operations that they carry out, it might be necessary for the DPO function to have a deputy/assistant DPO[49] and/or assisting staff (legal officers, IT officers, administrative assistants, etc.).[50]

71. Where appropriate and where compatible with the internal rules of the EUI, DPOs may be granted authority to manage staff supporting the DPO function within a distinct organisational entity (unit, sector, team, etc.). The implementing rules concerning the DPO[51] should clarify these arrangements.

72. All DPO tasks listed in Article 45 EUDPR must remain under the responsibility of the DPO and their team and must not be assigned to staff members who report elsewhere for those tasks.[52]

C. Data protection coordinators

73. In larger EUIs, it can also be useful to extend the data protection culture to all organisational parts, with the designation of data protection coordinators ('DPCs') in different services (e.g. Directorate-General). DPCs advise and assist their service in all data protection aspects and liaise with the DPO where appropriate.

74. The DPC should be chosen at an appropriate hierarchical level and according to their knowledge of the functioning of the EUI in general and particularly the service where they are appointed.

75. For EUIs with DPCs, the implementing rules concerning the DPO[53] should explicitly address the establishment of the DPC function, their designation process, their tasks and their interactions with the DPO.

3.2.4. Training

76. Article 44(2) EUDPR requires that EUIs provide resources for DPOs to maintain their expert knowledge.

77. Thus, it is the responsibility of EUIs to give their DPOs the opportunity to stay up to date with regard to developments within the field of data protection.[54] The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training and certification courses on data protection, meetings of the DPO network, EDPS-DPOs meetings, and other forms of professional development, such as participation in privacy fora, workshops, etc.

---

[49] On the deputy/assistant DPO, see section 2.6. *Continuity of the DPO function*.
[50] Article 44(5) EUDPR refers to the DPO 'and his or her staff'.
[51] See section 5. *Implementing rules concerning the DPO*.
[52] The data protection coordinators, if any, advise their own entity on data protection matters and are not as such part of the DPO team. See section 3.2.3., point C. *Data protection coordinators*.
[53] See section 5. *Implementing rules concerning the DPO*.
[54] See section 2.3. *Expertise and skills of the DPO* (Article 43(3) EUDPR).

78. Establishing a longer term of designation[55] and a minimum percentage of time to carry out their function also helps the DPO to build expertise in the field.

79. Moreover, the exponential advancement of artificial intelligence (AI) across all spheres of the society, including EU public administration, has a significant impact on the processing of personal data in EUIs. DPOs must be properly involved whenever AI systems process personal data.

80. In the context of the implementation by EUIs of generative AI systems that process personal data it is important to ensure that DPOs, within their role, advise and assist in an independent manner on the application of the Regulation, have a proper understanding of the lifecycle of the generative AI system that the EUI is considering to procure, design or implement and how it works. This means, obtaining information on when and how these systems process personal data, and how the input and output mechanisms work, as well as the decision-making processes implemented through the model.[56]

81. To be able to provide meaningful advice in this constantly evolving area, DPOs should receive comprehensive training and benefit from regular updates on the matter.

3.3. Independence of the DPO (Article 44(3)-(5) and (7) EUDPR)

82. The independence of the DPO is a cornerstone of effective data protection governance. It is directly linked to the exercise of the DPO's tasks and requires that the DPO operate free from instructions, undue influence or pressure, while enjoying direct and unhindered access to the controller. This autonomy enables the DPO to form and express their own opinions, provide impartial advice, and carry out their responsibilities without interference.

83. DPOs occupy a structurally complex position: they are part of the EUI while remaining functionally independent in the performance of their duties. This dual position allows them to monitor compliance from within the organisation and to intervene or advise at an early stage. The EUDPR therefore provides a set of guarantees designed to ensure the DPO's independence.

3.3.1. Absence of instructions (Article 44(3), first sentence EUDPR)

84. EUIs must ensure that the DPO does not receive any instructions regarding the exercise of their tasks.[57] This provision is paramount in ensuring independence of DPOs.

85. This prohibition covers not only explicit instructions from hierarchical superiors but also situations in which the DPO may feel indirectly pressured to compromise their independence. Such risks may arise, for example, where DPOs are employed under fixed-term contracts and perceive a link between their advice and contract renewal or extension. [58]

---

[55] See section 3.5. *Term of designation* (Article 44(8), first sentence, EUDPR)

[56] See EDPS supervisory guidance: Generative AI and the EUDPR. Orientations for ensuring data protection compliance when using Generative AI systems (28 Oct 2025).

[57] Article 44(3), 1st sentence EUDPR.

[58] The same concern goes for outsourced DPO.

86. Part-time DPOs may also face tensions between their DPO duties and other tasks, particularly where their appraisal focuses primarily on non-DPO functions.[59] To safeguard independence, the preferred organisational arrangement is to place the DPO outside any operational department, service, or unit. Where this is not feasible, any administrative placement must not affect the DPO's functional independence.

87. The DPO must retain sole responsibility and authority for the exercise of their tasks. The DPO should prepare and communicate their advice independently, and their advice must not be subject to any prior approval.

88. The EDPS encourages DPOs to develop their own working methods (objectives, annual work programme, annual report, etc.), which will serve to measure the performance of their work. The documents elaborated by the DPO to this effect should not require the approval of the management. Moreover, the DPO should be free to adjust their plans, in particular the audit and training plan, during the year as necessary. Otherwise, the independence of the DPO would be at risk.

3.3.2. No dismissal or penalisation for performing DPO tasks (Article 44(3) second sentence EUDPR)

89. To guarantee their independence, the DPO must not be dismissed or penalised by the controller or processor for performing their tasks.[60] This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.

90. Penalties are prohibited under the EUDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO.

> *For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.*

91. Penalties may take a variety of forms and may be direct or indirect. Penalisation could take the form of denial of benefits that other staff members receive, absence or delay of promotion, and any other type of discriminatory measures imposed on the DPO solely for performing their duties. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to their DPO activities.

92. DPOs should not suffer prejudice in their career development from the mere fact of being a DPO.

---

[59] See section 3.2.3., point A. *Full-time and part-time DPOs*.
[60] Article 44(3), 2nd sentence EUDPR.

93. The term 'dismissal includes, but is not limited to, the termination of the employment contract by the employer of the data protection officer.[61]

94. Dismissal or disciplinary sanctions for other legitimate reasons, such as serious misconduct, remain possible at any time.

95. The Court of Justice of the European Union (CJEU) has clarified that the requirement to refrain from dismissing or penalising the DPO for performing their duties must be regarded as essentially seeking to preserve the functional independence of the DPO and, therefore, to ensure that the data protection rules are effective. By contrast, that requirement is not intended to govern the overall employment relationship between a controller or a processor and staff members.62

96. Unlike the GDPR, the EUDPR contains specific provisions governing the dismissal of DPOs in EUIs, thereby providing enhanced protection for the DPO function, in particular by requiring the prior consent of the EDPS before a DPO may be dismissed.[63]

3.3.3. Direct reporting to the highest management level (Article 44(3), third sentence EUDPR)

97. The EUDPR requires that the DPO shall directly report to the highest management level of the controller or the processor.[64]

A. Direct reporting

98. The obligation 'to report' means 'to give an account on' or 'to be responsible to' (a superior). 'Direct reporting' means that, for the purposes of their DPO tasks, the DPO interacts with senior management in their EUI without intermediaries.

99. Direct reporting highlights that DPOs serve as an advisor to senior management, supporting and constructively assisting them in making informed decisions within the EUI. Direct reporting ensures that the top management is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller.[65]

100. Direct reporting may be implemented through various mechanisms, including:

101. EUIs should invite and actively involve (i.e. give them the possibility to submit their views, both orally and writing) the DPO in senior management meetings with agenda items involving data processing operations or issues.

102. Where a controller intends to adopt decisions that the DPO considers incompatible with the EUDPR and/or does not follow the DPO's advice on the matter, DPOs should have the possibility to express their dissenting opinion to those making the ultimate decision and,

---

61 EFTA Court, Judgment of of 16 December 2025, Rainer Silbernagl v. University of Liechstenstein, case E-5/25, paragraph 50 (regarding interpretation of Article 38(3) GDPR).

62 Judgment of 22 June 2022, Leistritz, C-534/20, ECLI:EU:C:2022:495, paragraph 28.

63 See section 3.6. *Dismissal of the DPO* (Article 44(8), second sentence, EUDPR).

64 Article 44(3), third sentence EUDPR.

65 Article 45(1)(a) EUDPR. See also section 4.2. *Advisory function* (Articles 45(1)(a), (d), (e) and (f) and 45(2), first sentence EUDPR).

where appropriate, inform the EDPS.[66] The possibility for the DPO to voice a contrary opinion is a critical safeguard for transparency and accountability in data protection governance.

103. DPOs should maintain regular communication, including meetings, with the senior management to update them on the ongoing data protection matters in the EUI.

104. DPOs should communicate their annual work programme (audit plan, training activities, etc.) to the senior management, and to adjust the plan during the year according to need.

105. DPOs should communicate periodic reports on the level of data protection compliance within the EUI to the senior management without approval by intermediaries.

B. Highest level of management

106. The 'highest management level' is not defined by the EUDPR and may differ across EUIs. The rule enshrined in the third sentence of Article 44(3) EUDPR aims to ensure that the DPO has access to those who have decision-making powers on data protection-related matters within the EUI.

107. The founding acts of some EUIs indicate the entity to which the DPO should directly report.[67] This must, however, not prevent the DPO from also reporting to other persons or entities that have decision-making powers within the EUI (e.g. Executive Director, Administrative Director, Director, Secretary-General, etc.).

108. Where the direct reporting line to the highest management level is not regulated in the founding act, the EUI's implementing rules concerning the DPO[68] should clarify the matter, to reinforce transparency and accountability within the EUI.

109. The DPO is a specific and independent function in EUIs. The EUI's organisation chart should duly reflect this, as well as the existence of a direct reporting line between the DPO and the highest management level of the EUI. This should be the case even though the DPO may assigned to a specific service for administrative purposes.[69]

110. The requirement to report to the highest management level does not affect the DPO's administrative attachment, on which the EUDPR is silent.[70] In this vein, 'direct reporting to the EUI's highest level management' does not necessarily mean that the entity to which the DPO reports should necessarily be the DPO's reporting officer within the meaning of the Staff

---

66 Article 41b(5) of the Europol Regulation, Article 38(4) of the Eurojust Regulation and Article 79(4) of the EPPO Regulation provide for an escalation procedure by the DPO when they consider that the data protection provisions have not been complied with.

67 Article 41a(3), second sentence, of the Europol Regulation provide that the DPO shall report directly to the Management Board; Article 37(3), third sentence of the Eurojust Regulation provides that the DPO shall report directly to the College in relation to operational personal data and to the Executive Board in relation to administrative data; Article 78(3), third sentence of the EPPO Regulation provides that the DPO shall directly report to the European Chief Prosecutor.

68 See section 5. *Implementing rules concerning the DPO*.

69 See section 3.3.1. *Absence of instructions* (Article 44(3), first sentence EUDPR).

70 On the administrative attachment of the DPO, see also section 3.3.1. *Absence of instructions* (Article 44(3), first sentence EUDPR).

Regulations, notably in relation to their annual appraisal.[71] Direct reporting and evaluation of performance are different things that do not follow the same rules.

111. However, the entity to whom the DPO reports in their data protection tasks, i.e. the highest management level of their EUI, must contribute to the annual appraisal of the DPO when it comes to the performance of their DPO duties. Furthermore, the evaluation of a DPO in the performance of their duties as DPO should be clearly distinguished from the evaluation of the performance of their other tasks, if any.

112. The EUI's implementing rules concerning the DPO[72] should clearly define the mechanisms for direct reporting and rules on the DPO appraisal, in particular when the DPO is administratively placed in an entity with other attributions than the data protection function.

3.3.4. Direct access to the DPO (Article 44(4) and (7) EUDPR)

113. Data subjects may contact the DPO in relation to all issues related to processing of their personal data and to the exercise of their rights under the EUDPR.[73]

114. Moreover, controllers and processors, the staff committee and more generally any individual may consult the DPO on any matter concerning the interpretation or application of the EUDPR, without them going through the official channels.[74]

115. In this context, the EUDPR specifies that no one shall suffer prejudice on account of a matter brought to the attention of the competent DPO alleging that a breach of the EUDPR has occurred.[75]

3.3.5. Confidentiality (Article 44(5) EUDPR)

116. The DPO and their staff are bound by secrecy or confidentiality concerning the performance of their tasks.[76] This obligation reinforces the DPO's independence and position within the organisation.

As a good practice, EUIs should provide secure communication channels for contacting the DPO, such as encrypted email or dedicated internal communication systems. DPOs should be able to choose appropriate communication tools and should demonstrate their commitment to protecting the identity of complainants where necessary.

3.4. No conflict of interests (Article 44(6) EUDPR)

117. According to Article 44(6) EUDPR, the DPO may fulfil other tasks and duties. However, EUIs must ensure that 'any such tasks and duties do not result in a conflict of interests'.

---

71 As regulated by Article 43 of the Staff Regulations.
72 See section 5. *Implementing rules concerning the DPO.*
73 Article 44(4) EUDPR.
74 Article 44(7), first sentence EUDPR. See also section 4.5. *Handling queries, complaints and other matters* (Articles 44(4) and (7) EUDPR and 45(2), second sentence, EUDPR).
75 Article 44(7), second sentence EUDPR.
76 Article 44(5) EUDPR.

118. To ensure the effectiveness of the DPO function, the DPO should operate with full independence and without any conflicting responsibilities. While additional tasks may be entrusted to the DPO, these must not hinder the performance of the tasks assigned under the EUDPR, including by depriving the DPO of the time necessary to perform them, nor may they give rise to a conflict of interests.

3.4.1. Definition

119. In terms of Article 44(6) EUDPR, a conflict of interests may arise where the DPO position is in conflict with other roles that the DPO may have in the EUI.[77] However, the EUDPR does not define the notion of 'conflict of interests' means in the context of the DPO. Guidance can be drawn from the case law of the Court of Justice of the European Union (CJEU) under the GDPR, which is applicable by analogy under the EUDPR. [78]

120. The CJEU has assessed the notion of conflict of interests of the DPO under the GDPR and found that while the DPO may be entrusted with performing tasks and duties other than DPO tasks and duties, they cannot be entrusted with 'performing tasks or duties which could impair the execution of the functions performed by the DPO', in order to 'preserve the functional independence of the DPO and, consequently, to ensure the effectiveness of the provisions of the GDPR.'[79]

121. Moreover, the CJEU takes the view that a conflict of interests may exist where a DPO is entrusted with other tasks or duties, which would result in them 'determining the objectives and methods of processing personal data on the part of the controller or its processor', which is a matter to be determined, 'case by case, on the basis of an assessment of all the relevant circumstances, in particular the organisational structure of the controller or its processor and in the light of all the applicable rules, including any policies of the controller or its processor.'[80]

3.4.2. Situations

A. DPO and (previous) controller

122. In line with the principles established by the CJEU, the DPO cannot hold a position within the EUI that leads them to determine the purposes and the means of the processing of personal data.

> *Positions that typically give rise to conflict of interests include senior management positions, Head of Human Resources (HR), or other middle management roles with operational control over data processing such as compliance, IT or medical service).*

---

[77] The concept of conflict of interests in this context is different from that of the Article 11a of the Staff Regulations. In the latter, a conflict of interests is defined as a situation where EUI staff members in the performance of their duties deal with a matter in which, directly or indirectly, they have 'a personal interest such as to impair their independence, and in particular, family and financial interests.'

[78] Recital 4 of the EUDPR.

[79] Judgment of 9 February 2023, X-FAB Dresden GmbH & Co, Case C-453/21, ECLI:EU:C:2023:79, paragraphs 40-42.

[80] Judgment of 9 February 2023, X-FAB Dresden GmbH & Co, Case C-453/21, ECLI:EU:C:2023:79, paragraphs 44-46.

123. A conflict of interests may also arise when the DPO is involved in a processing where they were previously involved as operational controller.

124. Even positions lower in the organisational hierarchy may give rise to conflicts where they involve determining the purposes and means of processing.

> *A conflict of interests may typically arise when a part-time DPO who belongs to the IT service must assess processing operations that they have designed; or when a DPO who is also part of the compliance team must assess compliance checks and related data processing that they have designed.*

125. Responsibility for ensuring compliance with the EUDPR under Article 26 EUDPR cannot be delegated to the DPO. Conferring such responsibility would amount to granting decision-making authority over the purposes and means of processing and would therefore constitute a conflict of interests.

B. DPO and agent before the Court of Justice of the European Union

126. The EDPS considers that the DPO must not represent the EUI before the General Court or Court of Justice of the European Union in any data protection case involving the EUI. Such representation would be incompatible with the independence of the DPO, even if they have not been previously involved in the case at any stage. Litigating for and acting on behalf of the institution before a Court in data protection related cases would jeopardise independence and impartiality of the DPO, not only in the case at hand, but also in general. This could potentially damage the perception of the DPO as independent within the EUI and would inevitably give rise to a conflict of interests. This consideration is particularly relevant where a member of the legal service is designated as DPO.

> *If the DPO is also a member of the legal team, organisational measures should be put in place to ensure a clear separation of functions, for example by using a dedicated functional mailbox for DPO matters, so that the rest of the organisation can clearly identify whether advice is provided in the DPO capacity or in a legal advisory role.*

C. DPO and representative of the Appointing Authority

127. Similar considerations apply where the application of data protection rules is at issue, such as the European Ombudsman's inquiries into alleged maladministration or appeals under Article 90(2) of the Staff Regulations. The DPO should in principle not be involved as a representative of the Appointing Authority in such cases. There is therefore a need to ensure that internal policies reflect this and that procedures are in place to ensure that the DPO is not called upon to represent the EUI in data protection related cases.

D. DPO who is otherwise directly involved in a data protection matter

128. A conflict of interest can still arise in other situations. One example is when a DPO acts as a data subject. This could happen if they submit a request to have access to their own personal data, or in the framework of an administrative inquiry. Other examples include disciplinary proceedings, requests for assistance under Article 24 of the Staff Regulations, or complaints under Article 90 of the Staff Regulations.

129. A conflict also arises when the DPO is directly involved in a matter, and this involvement prevents them from giving independent advice to their EUI. For example, where there is an administrative inquiry involving a member of their team.

130. Due to the specific organisational structure in each EUI, the existence of a potential conflict of interests should be considered case by case and the different duties must be evaluated separately.

3.4.3. Prevention and resolution

131. Article 44(6) EUDPR places responsibility on the controller to implement organisational measures that prevent conflict of interests. Such organisational measures can take various forms and be combined to achieve full efficiency.

132. As a first step, EUIs should identify positions and tasks that are inherently incompatible with the DPO function. Second, EUIs should have rules and procedures in place to manage situations of conflict of interest when they arise.

133. EUIs should either include rules to this effect in the implementing rules concerning the DPO[81] or establish a dedicated internal policy. They should define situations requiring the DPO to recuse themselves and establish alternative arrangements that preserve independence. Establishing clear boundaries and governance mechanisms will help preserve the independence and credibility of the DPO role across all operational contexts.

134. Vacancy notices for DPO positions or service contracts should clearly describe the scope of responsibilities and safeguards against conflicts of interests.

135. Appointing a deputy DPO is a further recommended measure, allowing another individual to assume responsibilities in situations where the DPO must recuse themselves. Where no deputy DPO exists, procedures should be established to designate another person, internal or external, who enjoys equivalent guarantees of independence.

136. Raising awareness (e.g. by providing training) of the DPO and the management on potential conflicts of interests and how to manage them is an organisational measure that may be efficient in preventing conflicts of interests from occurring. The objectives should be to remind the DPO that they cannot be both judge and party in matters where they have contributed operationally, and to raise awareness of the management about the need to have rules and policies in place to prevent conflicts of interests and to deal with them when they arise.

137. Another organisational measure could be to carry out an internal audit, aiming at verifying that the structure and functioning of the EUI guarantees the independence of the DPO function and absence of conflict of interests. Such an audit should however not cover the substance of the DPO's work (i.e. the content of the advice they provide), as this would risk undermining their independence.

---

[81] See section 5. *Implementing rules concerning the DPO*.

3.5. Term of designation (Article 44(8), first sentence, EUDPR)

138. Article 44(8) EUDPR stipulates that the DPO shall be appointed for a term of three to five years.[82] They are eligible for reappointment.[83]

139. The length of the mandate of the DPO is an important factor in ensuring their independence. The longer the mandate, the more this contributes to providing a guarantee to the DPO that they can carry out their function in an independent manner. The EDPS therefore recommends that EUI appoint DPOs for a term of five years whenever possible.

140. The term of designation should be specified in the implementing rules concerning the DPO.[84]

141. Where DPOs are employed by an EUI under temporary contracts, the contract duration must align with the full term of their designation as DPO.

> *Y is employed by EUI A as a contract agent and is designated DPO for a term of three years. The remaining duration of the contract must therefore be at least three years.*

142. The EUDPR does not provide any term of designation for the deputy DPO. The implementing rules on the DPO could nevertheless include rules on the deputy DPO, if any, including their term of designation.

3.6. Dismissal of the DPO (Article 44(8), second sentence, EUDPR)

143. A DPO may be dismissed[85] only from their post if two cumulative conditions are met: if they no longer fulfil the conditions required to perform their duties, and only with the consent of the EDPS.[86] Equivalent requirements apply to the DPOs of Europol, Eurojust and the EPPO under their respective legal frameworks.[87]

144. The requirement for prior consent by the EDPS constitutes an additional safeguard designed to preserve the functional independence of the DPO.

> *The EDPS invites any DPO who faces a dismissal against their will, and where the EUI does not appear to intend to comply with Article 44(8) EUDPR, to contact the EDPS without delay, whether formally or informally.*

---

[82] Article 41a(7) of the Europol Regulation, Article 36(4) of the Eurojust Regulation and Article 77(4) of the EPPO Regulation provide a designation term of four years.

[83] By exception, the DPO of Eurojust and the DPO of EPPO may be reappointed but their total term of office must not exceed eight years (Article 36(4) of the Eurojust Regulation and Article 77(4) of the EPPO Regulation).

[84] See section 5. *Implementing rules concerning the DPO*.

[85] On the concept of 'dismissal', see section 3.3.2. *No dismissal or penalisation for performing DPO tasks* (Article 44(3) second sentence EUDPR).

[86] Article 44(8), second sentence EUDPR.

[87] Article 41a(8) of the Europol Regulation, Article 36(4) of the Eurojust Regulation and Article 77(4) of the EPPO Regulation.

3.6.1. Substantial requirement: the DPO does no longer fulfil the conditions to perform their duties

145. Articles 43 and 44 EUDPR set out a number of conditions required to perform the DPO duties. These include in particular:

(a) professional qualities and expert knowledge in data protection law and practices (Article 43(3) EUDPR);

(b) ability to perform the tasks assigned to DPOs under the EUDPR (e.g. informing and advising, monitoring compliance, cooperating with the EDPS) (Article 45 EUDPR).

146. Article 44(8) EUDPR should be read in light of the prohibition under Article 44(3) EUDPR to dismiss or penalise DPOs for performing their tasks.[88] The CJEU has interpreted this provision as 'essentially seeking to preserve the functional independence of the data protection officer', and further specified that this provision 'is not intended to govern the overall employment relationship between a controller or a processor and staff members who are likely to be affected only incidentally, to the extent strictly necessary for the achievement of those objectives'.[89] The Court of Justice also clarified that the prohibition of the dismissal, by a controller or processor, of a DPO or of the imposition, by a controller or processor, of a penalty on him or her means that that officer must be protected against any decision terminating his or her duties, by which he or she would be placed at a disadvantage or which would constitute a penalty[90].

147. In another judgment, the CJEU found that each Member State is free to lay down more protective special provisions concerning the revocation of the DPO, provided that those provisions are compatible with EU law and, in particular, with the provisions of the GDPR that provides that the DPO shall not be dismissed or penalised for carrying out their tasks. The CJEU stated, however, that such increased protection cannot jeopardise the achievement of the objectives of the GDPR, which would be the case if it prevented any revocation of a DPO who no longer possesses the professional qualities required to carry out their tasks, or who does not perform those tasks in accordance with the provisions of the GDPR.[91] Thus, a rigid protection regime that would prevent dismissing a DPO who is unable, or no longer able, to perform their tasks with full independence due to a conflict of interest would undermine the EUI's ability to ensure a high level of protection of natural persons with regard to the processing of their personal data.

148. If the EUI identifies a risk of a conflict of interests between the DPO's tasks and the DPO's other functions, it is the controller's responsibility to eliminate that risk by adopting appropriate measures. However, this does not in itself justify dismissing the DPO. Dismissal should be considered only as a last resort, and only where the controller can demonstrate that no other corrective measure would adequately resolve the conflict of interests. The EUI should thus demonstrate to a satisfactory level to the EDPS why it would be necessary to dismiss the DPO to address the risk of conflict of interests, i.e. that there are no other means available to the EUI to remove the potential conflict of interests.

---

88 See section 3.3.2. *No dismissal or penalisation for performing DPO tasks* (Article 44(3) second sentence EUDPR).
89 Judgment of 22 June 2022, Leistritz, C-534/20, ECLI:EU:C:2022:495, paragraph 28.
90 Judgment of 22 June 2022, Leistritz, C-534/20, ECLI:EU:C:2022:495, paragraph 21.
91 Judgment of 9 February 2023, KISA, Case C-560/21, ECLI:EU:C:2023:81, paragraphs 25-29.

149. The EDPS has considered that consent can be given where the proposed dismissal of a DPO is not linked to the performance of their tasks as DPO and results from other legitimate grounds, such as the failure to carry out other professional duties, or comply with obligations under the Staff Regulations, which may both result in the termination of their employment contract. Given that the termination of the employment contract means that the DPO no longer fulfils the requirement set out in Article 43(4) EUDPR, they cannot remain in the position as DPO. In other words, where the grounds for dismissal are unrelated to the performance of the DPO duties and tasks, and do not undermine the independence and effective performance of DPO tasks within the EUI, the EDPS will not oppose the dismissal.

150. Organisational restructuring, elimination of the post, or incompatibility with managerial preferences can never be regarded as valid reasons to dismiss the DPO.

3.6.2. Formal requirement: Prior consent from the EDPS

151. Irrespective of the grounds invoked, EUIs must obtain the EDPS' prior consent before dismissing a DPO. This legal requirement is an important factor in ensuring the functional independence of the DPO. The obligation to obtain consent does not aim to interfere with the organisational autonomy of EUIs but serves to reinforce accountability through a specific requirement to demonstrate that the dismissal is in line with the provisions of the EUDPR on the DPO's independence.

152. The obligation to involve the EDPS applies whenever an EUI considers or intends to dismiss a DPO, irrespective of the underlying reasons. This ensures that Article 44(8) EUDPR has *effet utile* in light of Article 16(2) TFEU and Article 8(3) of the Charter of Fundamental Rights, and strengthens the overall effectiveness of supervision.[92]

153. Adopting an interpretation of Article 44(8) EUDPR to the contrary would effectively confer upon EUIs the discretion to determine by themselves whether to request the consent of the EDPS, based solely on their own assessment of the circumstances, which would risk undermining the procedural safeguards envisaged by the EUDPR. This could lead EUIs to attempt to circumvent Article 44(8) EUDPR by not providing (adequate) reasoning for the dismissal.

154. Failure to obtain prior consent may lead the EDPS to exercise corrective powers under Article 58(2) EUDPR.[93]

155. For the practical steps through which an EUI can obtain the EDPS' consent before dismissing its designated DPO, see the EDPS Decision adopting the Rules on the application of the requirement of prior consent by the EDPS for the dismissal of Data Protection Officers[94].

---

[92] Judgment of 21 June 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, paragraph 86: '(...) in accordance with a general principle of interpretation, an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law (judgment of 2 February 2021, Consob, C-481/19, EU:C:2021:84, paragraph 50 and the case-law cited).'

[93] See for example EDPS Decision 35/2025 and Decision 55/2025.

[94] Reference to the OJ once published.

3.7. Registration with the EDPS (Article 44(9) EUDPR)

156. Following designation, the DPO must be registered with the EDPS by the appointing EUI.[95] Registration should take the form of a formal communication to the EDPS enclosing the designation decision. That decision should specify the term of the designation and its starting date.

> *As a matter of good practice, the designation of a deputy DPO should be formally notified to the EDPS following the same procedure.*[96]

157. The designation of temporary DPOs should also be notified to the EDPS and include a deadline for the appointment of a permanent DPO. Such arrangements are, by definition, temporary and must not persist indefinitely.[97]

4. Tasks of the DPO

158. The DPO has a central role within the EUI. Owing to their familiarity with the organisation and their independent status, DPO play a crucial role in giving advice and helping solve data protection issues. The DPOs are unique since they will simultaneously act as advisor, educator and point of contact for competent authorities and data subjects.

159. Article 44(1) EUDPR reinforces the role of the DPO in requiring that data controllers involve them, properly and in a timely manner, in all issues, which relate to the protection of personal data.

160. Article 45 EUDPR assigns several tasks, duties and powers to the DPO.98 These should be further detailed in the implementing rules concerning the DPO adopted pursuant to Article 45(3) EUDPR.99

161. While DPOs are expected to perform the tasks described below, as well as those in relation to the EDPS set out below in Section 6[100], responsibility for ensuring that processing operations comply with the EUDPR remains with the controller.[101]

162. The autonomy conferred on DPOs under the EUDPR ensures their independence in the performance of their duties. However, this autonomy does not confer broad decision-making authority beyond the scope of their defined tasks. DPOs are empowered to take decisions and

---

95 Article 44(9) EUDPR.
96 Under Article 41a(9) of the Europol Regulation, the assistant DPO, if any, must be registered with the EDPS.
97 See section 2.6. *Continuity of the DPO function*.
98 Article 41b of the Europol Regulation, Article 38 of the Eurojust Regulation and Article 79 of the EPPO Regulation on the tasks of the DPO list additional tasks of the DPO. A number of these tasks are identical or similar to the tasks listed in Article 45 EUDPR, other are specific. See *Annex - Provisions on the DPO - Cross-reference table*.
99 See section 5. *Implementing rules concerning the DPO*.
100 See section 6. *Relation between the DPO and the EDPS*.
101 Article 26(1) EUDPR.

provide guidance strictly within the boundaries of their responsibilities as outlined in the EUDPR.

4.1. Information and awareness-raising function (Article 45(1)(a) and (c) EUDPR)

163. The DPO fulfils an awareness raising role and aims to promote a data protection culture within their EUI.

164. This implies both informing data controllers and processors of their obligations and responsibilities and ensuring that data subjects are informed of their rights and obligations pursuant to the EUDPR.[102] Awareness-raising can take the form of information notes to staff, training sessions, up-to-date data protection sections on the intranet and on the EUI website, data protection notices, etc. DPOs can include an awareness-raising point in their annual work programme.

4.2. Advisory function (Articles 45(1)(a), (d), (e) and (f) and 45(2), first sentence EUDPR)

165. DPOs shall advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the EUDPR and to other Union data protection provisions.[103] The DPO may make recommendations to the data controller for the practical improvement of data protection and advise them on matters concerning the application of data protection provisions.[104]

166. In addition to their general advisory role, the EUDPR specifically indicates that the DPO should provide advice in certain specific situations:

Personal data breaches

167. The DPO should advise, where requested, on the necessity for a notification or a communication of a personal data breach pursuant to Article 34 and 35 EUDPR.[105]

Data protection impact assessment

168. The DPO should provide advice, where requested, on data protection impact assessments ('DPIAs') and monitor their performance pursuant to Article 39 of the EUDPR.[106]

169. The responsibility for carrying out a DPIA rests with the controller, not with the DPO. However, the DPO can play a very important and useful role in assisting the data controller in advising whether to carry out a DPIA, what methodology to use, what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights

---

[102] Article 45(1)(a), (b) and (c) EUDPR.
[103] Article 45(1)(a) EUDPR.
[104] Article 45(2) EUDPR. See also section 4.5. *Handling queries, complaints and other matters* (Articles 44(4) and (7) EUDPR and 45(2), second sentence, EUDPR)
[105] Article 45(1)(d) EUDPR. Moreover, Article 34(5) EUDPR provides that the controller shall inform the DPO about personal data breaches.
[106] Article 39(2) EUDPR (controller's obligation to consult the DPO on DPIAs) and Article 45(1)(e) EUDPR (DPO's corresponding task).

and interests of the data subjects, whether the DPIA has been correctly carried out, and whether its conclusions are in compliance with the EUDPR.

Prior consultation

170. The DPO should advise, where requested, on the need for prior consultation of the EDPS in accordance with Article 40 of the EUDPR.[107] Similarly, as for DPIAs, the DPO can play an essential role in this regard, given their expertise and experience in assessing sensitive processing operations.

171. Furthermore, the EUDPR explicitly lays down that the DPO must consult with the EDPS in case of doubt as to the need for DPIA and for prior consultation.[108]

4.3. Cooperative function (Article 45(1)(g) EUDPR)

172. The DPO has the task of responding to requests from the EDPS, in coordination with the respective controllers within the EU. In addition, within the sphere of their competence, the DPO cooperates and consults with the EDPS at the latter's request or on their own initiative.[109]

173. This task highlights the fact that the DPO facilitates cooperation between the EDPS and their EUI, notably in the framework of investigations, complaint handling, DPIAs and prior consultations. The DPO's internal knowledge of the EUI enables them to identify relevant interlocutors and provide contextual information. The DPO may also be aware, and duly inform the EDPS, of recent developments likely to affect the protection of personal data.

174. As a general rule, the DPO should be copied on all communications between the EUI and the EDPS relating to data protection matters.

4.4. Monitoring compliance (Article 45(1)(b) and (h) and (2) EUDPR)

175. The DPO shall ensure in an independent manner the internal application of the EUDPR and monitor compliance with the EUDPR,[110] with other applicable EU law containing data protection provisions, and with the policies of the data controller or processor in relation to data protection, including assigning responsibilities, raising awareness, and training of staff involved in processing operations, and the related audits.

176. The DPO is also tasked with ensuring that the rights and freedoms of data subjects are not adversely affected by processing operations.[111]

177. To monitor compliance, DPOs may develop templates for use by controllers based on which they can monitor compliance with the EUDPR and make recommendations.[112] DPOs can also develop internal policies and FAQs on thematic topics to provide guidance to data controllers.

---

[107] Article 45(1)(f) EUDPR. Article 40(1), last sentence EUDPR also provides that the controller must consult the DPO on the need for prior consultation.
[108] Article 45(1)(e),(f) EUDPR.
[109] Article 45(1)(g) EUDPR
[110] Article 45(1)(b) EUDPR
[111] Article 45(1)(h) EUDPR
[112] Article 45(2) EUDPR.

As a good practice, some DPOs collect and monitor internal data protection metrics (number of consultations, personal data breaches, EDPS complaints, data subject requests, etc.). Such metrics may serve as indicators of the effectiveness of data protection implementation within the EUI and support reporting on DPO activities.

4.5. Handling queries, complaints and other matters (Articles 44(4) and (7) EUDPR and 45(2), second sentence, EUDPR)

178. Data subjects may contact the DPO about issues related to processing of their personal data and the exercise of their rights.[113] In addition, the DPOs may, on their own initiative or at the request of the data controller or the processor, the staff committee, or any individual,[114] investigate matters and occurrences directly relating to their tasks and which come to their notice, and report back to the person who commissioned the investigation, or to the data controller or processor.[115]

179. The staff committee and all services of the EUI should cooperate closely with the DPO in cases of an alleged breach of data protection rules and ensure that the DPO is duly informed and consulted.

180. For these purposes, the DPO is granted with investigative powers and can handle queries or complaints submitted by members of staff or the public.[116] The DPO must have access to all personal data and to information necessary for the performance of their tasks.[117]

181. For reasons of efficiency, the EDPS encourages that DPOs investigate and handle complaints. As a general rule, the EDPS therefore encourages complainants to first contact the DPO before lodging a complaint with the EDPS. The DPO's proximity to the organisation and to data subjects places them in a favourable position to address issues promptly. This does not however prevent data subjects from directly addressing the EDPS under Articles 63(1) and 68 EUDPR.

182. The implementing rules concerning the DPO[118] should further specify the exercise of the DPO's investigative powers, while preserving the DPO's independence and confidentiality, including vis-à-vis management.[119]

4.6. Other assignments

183. EUIs sometimes assign other tasks than those listed in Article 45 EUDPR to their DPO.

---

[113] Article 44(4) EUDPR. See also section 3.3.4. *Direct access to the DPO* (Article 44(4) and (7) EUDPR).
[114] Article 44(7), first sentence, EUDPR.
[115] Article 45(2) EUDPR. See also Article 44(7) EUDPR and section 3.3.4. *Direct access to the DPO* (Article 44(4) and (7) EUDPR).
[116] Article 45(2), second sentence EUDPR.
[117] Article 44(2) EUDPR.
[118] Section 5. *Implementing rules concerning the DPO.*
[119] See section 3.3.5. *Confidentiality* (Article 44(5) EUDPR).

184. For example, while the responsibility for maintaining records of processing activities lies with the controller and/or the processor,[120] DPOs often maintain a central register of processing operations based on information provided by responsible services.

185. The EDPS recommends that EUIs centralise their records in a public register kept by the DPO.[121] Such a record helps the DPOs to perform their tasks of monitoring compliance, informing and advising the controller or the processor. The record should also be seen as 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 measure. However, responsibility for the accuracy and completeness of the records remains with the controller.

186. In many EUIs, the DPO also coordinates and handles data subject requests for access, rectification, and erasure.[122] While data subjects may contact the DPO about the exercise of their rights,[123] and the DPO often supports controllers in dealing with data subject requests, the obligations to comply with data subject rights lies with the controller.

4.7. Enforcement

187. Although the DPO is responsible for monitoring compliance and handling complaints, their enforcement powers are limited. The DPO does not have sanctioning authority.

188. Where necessary, the DPO may bring instances of non-compliance under the EUDPR to the attention of the highest management level of their EUI.[124] This may result in a possible application of Article 69 of the EUDPR.[125]

189. The DPO always has the possibility to inform the EDPS on any matter of concern, if necessary, without informing their EUI.[126]

---

[120] Article 31 EUDPR.

[121] EDPS Toolkit - Accountability on the ground (Feb. 2018), p. 7.

[122] See EDPS survey report on the position of the DPO (18 Jan 2024), reply to question 14: 41 of the 69 respondents indicated that they were in charge of fulfilling data subject requests.

[123] Article 44(4) EUDPR. See section 3.3.4. *Direct access to the DPO* (Article 44(4) and (7) EUDPR).

[124] See section 3.3.3. *Direct reporting to the highest management level* (Article 44(3), third sentence EUDPR).

[125] Article 69 Sanctions : 'Where an official or other servant of the Union fails to comply with the obligations laid down in this Regulation, whether intentionally or through negligence on his or her part, the official or other servant concerned shall be liable to disciplinary or other action, in accordance with the rules and procedures laid down in the Staff Regulations.'

[126] See section 6.2. *Enforcement*.

5. Implementing rules concerning the DPO

5.1. Obligation to adopt implementing rules concerning the DPO (Article 45(3) EUDPR)

190. EUIs are required adopt implementing rules concerning the DPO.[127] These implementing rules are an important instrument for reinforcing the involvement, position and effectiveness of the DPO function, considering the specific characteristics of each EUI.

5.2. Content of the implementing rules

191. The EUI's implementing rules shall in particular concern the tasks, duties and powers of the DPO.128

192. The implementing rules should not merely reproduce the wording of the EUDPR concerning the DPO. Rather, they should further specify and operationalise those provisions by laying down tailored internal rules adapted to the organisational structure, mandate and activities of the EUI in question.

193. In particular, the implementing rules should address:[129]

- the term of designation of the DPO;
- the appointing authority and the reporting line for the performance of DPO tasks;
- the mechanisms ensuring direct reporting to the highest management level;
- arrangements for the appraisal of the DPO, including clear separation between the evaluation of DPO duties and other functions, if any;
- whether the DPO is supported by a deputy, assistant or team, and the organisation of that support;
- measures ensuring continuity of the DPO function in cases of temporary absence or incapacity;
- the establishment, designation and role of Data Protection Coordinators and their interaction with the DPO;
- measures for the prevention and management of conflicts of interests;
- the practical exercise of the DPO's investigative powers.

194. By providing clarity on these elements, implementing rules concerning the DPO contribute to transparency, accountability and legal certainty within the EUI.

---

[127] Article 45(3), first sentence EUDPR.
[128] Article 45(3), second sentence EUDPR.
[129] Article 41a(5) of the Europol Regulation, Article 37(5) of the Eurojust Regulation and Article 78(5) of the EPPO Regulation provide that the implementing rules shall in particular concern the selection procedure for the DPO position, their dismissal, tasks, duties and powers, and safeguards for their independence.

5.3. Elaboration and adoption process

195. The DPO should take the lead in drafting the implementing rules and be closely associated to their adoption process. This reflects the DPO's expertise and central role in ensuring the internal application of the EUDPR.

196. Pursuant to Article 41(1) EUDPR, EUIs must inform the EDPS 'when drawing up administrative measures and internal rules relating to the processing of personal data'. The implementing rules concerning the DPO are internal rules relating to the processing of personal data, falling within the scope of Article 41(1) EUDPR. As such, they must be submitted to the EDPS before their adoption.[130] The EDPS publishes its Supervisory Opinions on implementing rules concerning the DPO on its website.[131]

197. The implementing rules should be subsequently adopted by the EUI's highest level of management.

6. Relation between the DPO and the EDPS

198. An effective working relationship between the DPO and the EDPS is essential to ensure the internal application of the EUDPR within EUIs. The DPO must not be perceived as an 'agent' of the EDPS, but as an integral part of the EUI in which they operate. This proximity to the organisation places the DPO in a particularly effective position to ensure compliance from within and to intervene or provide advice at an early stage.

199. At the same time the EDPS can offer valuable support to DPOs in the performance of their function.

200. The EDPS therefore endorses the continuation and strengthening of close cooperation between DPOs and the EDPS, as this collaboration contributes directly to the effective protection of personal data within EUIs.

6.1. Ensuring application

201. Ensuring application notably begins by raising awareness. As outlined above, the DPO plays a central role in developing internal knowledge and understanding of data protection obligations within the EUI. The EDPS welcomes this preventive approach, which promotes compliance through guidance and support rather than through enforcement alone.

202. The DPO also provides advice to the EUI on practical recommendations for improvement of data protection within the EUI or concerning the interpretation or application of the EUDPR.[132] This advisory function complements that of the EDPS which advises all EUIs on

[130] Such involvement of the EDPS should be limited to drafts that have been finalised internally and should not take place in relation to versions that have not yet been approved.
[131] https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/supervisory-opinions_en
[132] Article 45(2) EUDPR.

administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data.[133]

203. In practice, the EDPS is frequently consulted by DPOs on specific data protection issues through supervisory consultations. The EDPS provides guidance on a wide range of topics and, as a general rule, publishes its supervisory opinions and other relevant resources on its website for the benefit of all EUIs.

204. Bi-annual meetings between the EDPS and the DPO network constitute an essential forum for fostering consistent application of EU data protection law across EUIs. These meetings provide a structured environment for the exchange of best practices, discussion of common challenges, and alignment on emerging issues in a rapidly evolving digital landscape.

205. Beyond the bi-annual meetings, the DPO network serves as a collaborative platform to foster dialogue, cooperation and knowledge sharing between the EDPS and the DPOs to ensure consistent compliance with the EUDPR within the EUIs. As such, the network plays a pivotal role in strengthening compliance with data protection laws and promoting a unified approach to safeguarding personal data across the EU's administrative framework.

206. Over the years, the EDPS has launched several initiatives that aim at reinforcing its support to the DPO network. In particular, the EDPS has centralised contacts with the DPO network by designating a member of its staff as DPO network contact point. It has also put in place the 'DPO support group' a group composed of six to ten rotating DPOs who help preparing the EDPS-DPOs meeting in collaboration with the EDPS.

207. Additional EDPS initiatives include thematic roundtables with smaller groups of DPOs, presentations on EDPS decisions of broader relevance, targeted training sessions upon request, and the dissemination of the monthly "Quick News for DPOs" newsletter, which provides practical updates and insights.

6.2. Enforcement

208. DPOs have limited powers of enforcement under the EUDPR. The EDPS contributes to ensuring compliance with the EUDPR through the exercise of its supervisory and corrective powers, including prior consultations, data protection audits, complaint handling and investigations.

209. The handling of complaints and queries by the DPO as regards their EUI is encouraged, particularly as a first phase of investigation and resolution.[134] The EDPS therefore considers it good practice for DPOs to attempt to investigate and resolve complaints internally before referring them to the EDPS.

210. The DPO should nevertheless consult the EDPS whenever they have doubts on the procedure or substance of complaints. Given the limited enforcement powers of DPOs, certain matters may also need to be escalated to the EDPS for support.

---

[133] Article 57(1)(g) EUDPR.

[134] See section 4.5. *Handling queries, complaints and other matters* (Articles 44(4) and (7) EUDPR and 45(2), second sentence, EUDPR).

211. In certain sensitive cases where the DPO might fear repercussions from their EUI in connection with a complaint, it may be preferable for the EDPS to handle the complaint directly or to open an own-initiative investigation.

212. Data subjects may always lodge a complaint directly with the EDPS under Articles 63(1) and 68 EUDPR, without being required to approach the DPO or the EUI first. In exercising its supervisory and enforcement powers, the EDPS thereby reinforces the role of the DPO by providing an external and independent enforcement framework that supports the DPO's advice within the institution. In this context, the DPO acts as a key interlocutor for the EDPS, providing relevant information and facilitating appropriate follow-up to the measures adopted by the EDPS in decisions taken following a complaint or an own-initiative investigation.

213. To ensure effective cooperation and transparency, the DPO is copied on all communications with the EUI in the context of supervisory and enforcement activities and is thus kept fully informed of the EDPS's actions and their outcome.

6.3. Measuring effectiveness

214. The EDPS sees DPOs as valuable partners to when measuring the effectiveness of the implementation of the data protection requirements and evaluate progress in this area. The EDPS encourages DPOs to develop their own tools for measuring performance of internal data protection supervision. This will help them to measure the state of implementation of the EUDPR within the EUI.

215. Some EUIs have adopted implementing rules under Article 45(3) EUDPR providing for the involvement of the EDPS in the evaluation of the DPO's work. The EDPS is not, however, in a position to assess the DPO's day-to-day work. Any input requested from the EDPS based on such implementing rules should therefore be strictly limited to aspects involving direct interaction with the EDPS, such as participation in working groups, audits, or supervisory activities.

Annex - Provisions on the DPO - Cross-reference table

	EUDPR	Europol Regulation	Eurojust Regulation	EPPO Regulation
Designation				
Mandatory DPO	Art. 43(1)	Art. 41(1)	Art. 36(1), 1st sentence	Art. 77(1), 1st sentence
Shared DPO	Art. 43(2)			
Professional qualities	Art. 43(3)	Art. 41(2)	Art. 36(2)	Art. 77(2)
Staff member or external	Art. 43(4)	Art. 41(1)	Art. 36(1), 2nd sentence	Art. 77(1), 2nd sentence
Publication of contact details	Art. 43(5)	Art. 41(5)	Art. 36(5)	Art. 77(5)
Position				
Involvement	Art. 44(1)	Art. 41a(1)	Art. 37(1)	Art. 78(1)
Necessary resources, access to personal data and expert knowledge maintenance	Art. 44(2)	Art. 41a(2) and Art. 41b(4)	Art. 37(2) and 38(3)	Art. 78(2), 78(6) and 79(3)
No instructions	Art. 44(3), 1st sentence	Art. 41a(3), 1st sentence	Art. 36(1), 3rd sentence and 37(3), 1st sentence	Art. 77(1), 3rd sentence and 78(3), 1st sentence
No penalisation or dismissal	Art. 44(3), 2nd sentence	Art. 41(4)	Art. 37(3), 2nd sentence	Art. 78(3), 2nd sentence

Reporting to highest management level	Art. 44(3), 3rd sentence	Art. 41a(3), 2nd sentence	Art. 37(3), 3rd sentence	Art. 78(3), 3rd sentence
Contact for data subjects	Art. 44(4)	Art. 41a(4), 1st sentence	Art. 37(4)	Art. 78(4)
Confidentiality	Art. 44(5)	Art. 41a(6)	Art.37(6)	Art. 78(7)
Absence of conflict of interests	Art. 44(6)	Art. 41(3)	Art. 36(3)	Art. 77(3)
Consultation by controller, processor, staff committee and any individual	Art. 44(7), 1st sentence		Art. 37(7), 1st sentence	
No prejudice on account of a matter brought to the DPO	Art. 44(7), 2nd sentence	Art. 41a(4), 2nd sentence	Art. 37(7), 2nd sentence	
Term of designation	Art. 44(8), 1st sentence	Art. 41a(7)	Art. 36(4), 1st sentence	Art. 77(4), 1st sentence
Dismissal	Art. 44(8), 2nd sentence	Art. 41a(8)	Art. 36(4), 2nd sentence	Art. 77(4), 2nd sentence
Registration with EDPS	Art. 44(9)	Art. 41a(9)	Art. 37(8)	Art. 77(5)
Assistant DPO		Art. 41a(2), 2nd sentence, Art. 41a(9) and Art. 41a(10)		
Tasks				
Inform and advise	Art. 45(1)(a)	Art. 41b(b)	Art. 38(1)(b)	Art. 79(1)(b)

Ensure application and monitor compliance	Art. 45(1)(b)	Art. 41b(a)	Art. 38(1)(a)	Art. 79(1)(a)
Ensure data subject information about their rights	Art. 45(1)(c)	Art. 41b(f)	Art. 38(1)(g)	Art. 79(1)(g)
Provide advice on notification/communication of personal data breaches	Art. 45(1)(d)	Art. 41b(d)	Art. 38(1)(i)	
Keep a register of data breaches		Art. 41b(d)		
Provide advice on and monitor DPIA	Art. 45(1)(e)	Art. 41b(c)	Art. 38(1)(c)	Art. 79(1)(c)
Provide advice on need for prior consultation	Art. 45(1)(f)			
Respond to EDPS' requests / cooperate with EDPS	Art. 45(1)(g)	Art. 41b(h)	Art. 38(1)(f)	Art. 79(1)(f)
Ensure that rights and freedoms of data subjects are not adversely affected	Art. 45(1)(h)	Art. 41b(l)		
Make recommendations to and advise controller/ processor; investigate matters	Art. 45(2)	Art. 41b(2)		
Keep a record of (transmission,) transfer and receipt of personal data		Art. 41b(e)	Art. 38(1)(d)	Art. 78(1)(d)
Cooperate with staff responsible for procedures,		Art. 41b(g)	Art. 38(1)(e)	Art. 79(1)(e)

training and advice on data processing				
Cooperate with competent authorities of Member States		Art. 41b(i)		
Act as contact point for EDPS including on prior consultations and consult EDPS		Art. 41b(j)	Art. 38(1)(h)	Art. 79(1)(h)
Prepare annual report communicated to management and EDPS		Art. 41b(k)	Art. 38(1)(j)	Art. 79(1)(i)
Carry out functions under EUDPR with regard to administrative personal data		Art. 41b(3)	Art. 38(2)	Art. 79(2)
Escalate matters to highest management and EDPS		Art. 41b(5)	Art. 38(4)	Art. 79(4)
Implementing rules on the DPO				
	Art. 45(3)	Art. 41a(5)	Art. 37(5)	Art. 78(5)
Supervision by the EDPS				
	Art. 52(3)	Art. 43(1)	Art. 40(1)	Art. 85(1)