



Decision No 11-2024 adopting implementing rules concerning the Data Protection Officer pursuant to Article 45(3) of Regulation (EU) 2018/1725

THE EUROPEAN COURT OF AUDITORS

HAVING REGARD TO Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (the “Regulation”), and in particular Article 45(3) thereof;

HAVING REGARD TO the deliberations of the Court at its meeting of 8 February 2024, on the basis of DEC 016/24;

WHEREAS the Regulation sets out the data protection principles and rules applicable to the EU institutions, bodies, offices and agencies, and provides for the designation by each Union institution or body of a Data Protection Officer (DPO);

WHEREAS pursuant to Article 45(3) of the Regulation, each Union institution or body shall adopt further implementing rules concerning the DPO. The implementing rules shall in particular concern the tasks, duties and powers of the DPO;

WHEREAS it is necessary to update certain provisions to clarify specific terms;

HAS DECIDED:

Section I – General provisions

Article 1 Subject matter and scope

1. This Decision defines the rules concerning the DPO, pursuant to Article 45(3) of the Regulation. It also sets out rules and procedures for the application of the Regulation by the Court through the allocation of responsibilities internally.

2. The Decision applies to all activities relating to the processing of personal data by or on behalf of the Court that are covered by the Regulation. It also lays down internal rules relating to the establishment of internal data protection roles.

Article 2 Definitions

For the purposes of this Decision and without prejudice to the definitions provided by the Regulation:

1. “Controller” means the Court, which shall be considered as the controller within the meaning of Article 3(8) of the Regulation;
2. “Internal controller(s)” means the Court’s internal organisational entities, such as the chambers, directorates and departments, including the various committees, groups and panels;
3. “Designated person(s)” means the person(s) entrusted with data protection-related responsibilities¹ for data processing operations assigned to them by the Court or by an internal controller;
4. “Data protection coordinator(s)” (DPC(s)) means the staff member appointed by the Court or the internal controllers to assist them in all aspects of the protection of personal data.

A detailed and regularly updated guide *Data protection roles at the ECA* further sets out the role of the designated persons and data protection coordinators.

Section II – Data Protection Officer

Article 3 Designation, status and independence

1. The DPO shall be a staff member of the Court. He or she shall act independently and possess the necessary professional qualifications to be able to fulfil the tasks and duties referred to in Article 5 of this Decision.
2. The term of office of the DPO shall be five years, renewable for further periods of five years. For administrative purposes, the DPO shall be attached to the Secretariat-General, reporting directly to the Secretary-General. In this context, the DPO shall participate in preparing the Annual Work Plan of the Secretary-General.
3. The appointment of the DPO shall be communicated officially to all staff to ensure that the DPO function is known within the Court. The name and the contact details of the DPO shall be published on the Court’s intranet and organisational charts. The DPO’s functional e-mail address shall be included in the information to be provided by the Court or the internal controllers to data subjects.

¹ Data protection-related responsibilities include validation of the records of processing activities, approval of privacy statements or others.

4. The DPO may be dismissed with the consent of the European Data Protection Supervisor (the “EDPS”) if the DPO no longer fulfils the conditions required for the performance of the DPO’s duties, or at the request of the DPO for reasons that do not compromise the exercise of the DPO function.
5. The Court shall support the DPO in performing the tasks and duties referred to in Article 5 by providing the financial resources, infrastructure and staff necessary to carry out those tasks. Such support may include, but shall not be limited to, the following measures:
 - (i) if necessary, ensuring the DPO is given support by other Court services, such as the Legal Service, IT, the Internal Audit Service, the Information Security Officer, and the Data Protection Coordinators;
 - (ii) ensuring that the DPO maintains expert knowledge and has access to continuous relevant training on data protection and other forms of professional development.
6. The DPO shall not suffer any prejudice because of the performance of their duties.

Article 4 Conflicts of interest

1. Should the DPO fulfil other tasks and duties, the Secretary-General shall ensure that these other tasks and duties do not result in a conflict of interest. Like any other official, the DPO needs to report any potential conflict of interest, as laid down in the ECA’s ethical rules.
2. Evaluation of the DPO in the performance of their duties as DPO shall not be related in any way to the performance of other tasks.

Article 5 Tasks and duties

1. The DPO shall promote a culture of protection of personal data within the Court. He or she shall ensure that the designated person(s), processors and data subjects are informed of their rights, obligations and responsibilities. For these purposes, the DPO may initiate staff information notes, training sessions, data protection notices and other information and awareness-raising measures.
2. The DPO shall monitor compliance of the Court with the Regulation, other applicable Union law containing data protection provisions and the Court’s policies in relation to the protection of personal data. As part of these monitoring duties, the DPO may:
 - (i) collect information to identify processing activities;
 - (ii) analyse and check the compliance of processing activities;
 - (iii) inform, advise and issue recommendations to the Court, designated person(s), or processor(s);
 - (iv) carry out inspections and audits.
3. The DPO shall assist the designated persons in preparing the records of processing activities. The designated persons shall assist the DPO in the performance of the DPO’s duties and provide the information which the DPO requests without undue delay.

4. Pursuant to Article 31(5) of the Regulation and building on the records provided by the designated persons, the DPO shall keep a register of the processing activities carried out by the Court. The DPO shall make the register publicly accessible.
5. The DPO shall help the designated persons to assess the data protection risks of the processing activities under their responsibility. The DPO shall provide advice and assist the designated persons when carrying out a data protection impact assessment (DPIA). The DPO will also advise on what methodology to use and contribute to selecting the safeguards to apply to mitigate the risks to the rights and freedoms of the data subjects, as well as the correct implementation of the DPIA.
6. In the event of a personal data breach, the person who identifies a breach or suspects a breach shall report the incident to the DPO without undue delay, including where there are doubts on whether personal data are affected by the security breach. The personal data breach procedure describes in detail how to fulfil this obligation.
7. The DPO shall keep an internal register of personal data breaches within the meaning of Article 34(6) of the Regulation.
8. The DPO shall advise as regards the necessity for a notification or a communication of a personal data breach pursuant to Articles 34 and 35 of the Regulation.
9. The DPO shall advise the designated persons about the need for prior consultation of the EDPS in accordance with Article 40 of the Regulation. The DPO shall consult the EDPS in case of doubt as to the need for a prior consultation.
10. The DPO shall ensure that the designated persons inform data subjects of their rights and obligations pursuant to the Regulation in the context of the processing activities for which they are responsible.
11. The DPO shall reply to questions and handle complaints from data subjects concerning data protection at the Court. Data subjects should in the first instance address their questions or complaints to the DPO, without prejudice to their right to contact the EDPS directly. The DPO may keep a confidential and anonymous inventory of requests from individuals that wish to reveal their identity only to the DPO when lodging requests or complaints. This inventory shall serve as a performance indicator to measure compliance with the Regulation. Requests pursuant to Articles 17 to 24 of the Regulation may not remain anonymous.
12. For processing operations on personal data for which they are themselves responsible, the DPO shall act as a designated person, acting under the Court's direct control or authority.
13. Without prejudice to the DPO's duties concerning cooperation with the EDPS pursuant to the Regulation, the DPO shall respond to requests received from the EDPS in relation to complaints and during EDPS inspections.
14. If the DPO deems it appropriate to do so, they shall inform the EDPS of any new developments at the Court relevant to the Court's compliance with data protection rules.

15. In addition to the above tasks, the DPO shall:

- (i) submit an annual activity report to the Secretary-General, who shall forward it to the Administrative Committee and the Court for information. This report shall be published on the Court's intranet and taken into account in the context of the DPO's annual performance appraisal;
- (ii) cooperate with the DPOs of other EU institutions and bodies in carrying out their functions, in particular by exchanging experiences and best practices through working groups and participation in the dedicated DPO network² or other inter-institutional networks;
- (iii) where possible, exchange experience and practices with DPOs from other organisations;
- (iv) be consulted before deciding whether a document which contains personal data that have been requested should be released pursuant to Decision No 37-2023 regarding public access to Court documents.

16. The DPO shall report any breach of the Regulation to the Secretary-General or the President, depending on who is responsible as Appointing Authority.

Article 6 Powers of the DPO

1. In performing their DPO tasks and duties, and without prejudice to the powers conferred by the Regulation, the DPO:
 - (i) may, in the event of disagreement with any designated person or processor on the interpretation or implementation of the Regulation, inform the Appointing Authority before referring the matter to the EDPS;
 - (ii) shall, where necessary, have access to the data forming the subject matter of processing operations on personal data, and to all premises, data-processing installations and data carriers, including those of processors;
 - (iii) shall be responsible for the initial decision on whether or not to release a document held by the DPO following a request for access under Decision No 37-2023 regarding public access to Court documents.
2. When making recommendations and rendering advice, the DPO may:
 - (i) call upon the designated persons or the processors to comply with the data subject's request for the exercise of their rights pursuant to the Regulation;
 - (ii) issue warnings to the designated person concerned and processor(s) when a processing operation infringes the Regulation, and call upon them to bring processing operations into compliance, where appropriate, in a specified manner and within a specified period;

² The DPO network is composed of the DPOs of EU institutions and bodies.

- (iii) call upon any designated person or any processor to suspend data flows to a recipient in a Member State, third country or international organisation;
- (iv) request the designated person concerned or the processor to report within a set deadline to the DPO on the follow-up given to the DPO's recommendation or advice;
- (v) bring to the attention of the Appointing Authority, any designated person or processor, in order to comply with the obligations under the Regulation and this Decision.

Article 7 Investigation procedure

1. Any individual may bring to the attention of the DPO a matter alleging that a breach of the provisions of the Regulation has taken place, or requests that the DPO investigate matters and occurrences directly relating to the DPO's tasks.
2. The requests for an investigation must be sent to the DPO in writing. Within 10 working days of receipt, the DPO shall send an acknowledgment of receipt to the person who commissioned the investigation and verify whether the request should be treated as confidential. In the event of manifest abuse of the right to request an investigation, for example where it is repetitive, inappropriate and/or pointless, the DPO shall inform the requester that the request is not being pursued and give an account of the reasons or shall not be obliged to report to the applicant any further.
3. If the requester is a data subject asking for an investigation into the processing of their personal data, or if the requester acts on behalf of the data subject concerned, the DPO must, to the extent possible, ensure the confidentiality of the request, unless the data subject concerned gives their unambiguous consent for the request to be handled otherwise.
4. The DPO shall request a written statement on the matter from the designated person concerned for the data processing activity in question. The designated person shall provide a response to the DPO within 10 working days. The DPO may request complementary information from the designated person concerned and/or from other parties within 10 working days.
5. The DPO shall report to the person who requested the investigation no later than one month following the receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests.

Article 8 Audit of data protection aspects

1. In the performance of the DPO's task of promoting and monitoring compliance with the Regulation, the DPO shall carry out independent audits of the processing of personal data to detect breaches or potential breaches of compliance, and recommend any required changes in the Court's control, policy and procedure concerning data protection.
2. The DPO shall, in collaboration with the Internal Audit Service, establish a compliance audit programme based on the type of personal data processed and the risk for the persons concerned (data subjects). The scope of the audit shall be defined by the DPO prior to the audit.

3. The audit shall include, but shall not be limited to, compliance with the requirements of the Regulation, with other applicable EU law containing data protection provisions and with the policies of the Court or its processors in relation to the protection of personal data. The audit may focus on general issues such as whether the Court has implemented policies and procedures to regulate the processing of personal data and whether that processing is carried out in accordance with such policies and procedures, or on any specific aspect of personal data processing at the Court.
4. Before carrying out an audit, the DPO shall inform the designated person concerned, who shall assist the DPO in the performance of this task and provide the DPO with any relevant information without undue delay.
5. The audit process shall provide an opportunity for the designated person concerned to respond to the observations and recommendations made by the DPO before the latter finalises the audit findings.
6. Following the completion of each audit, the DPO shall submit their findings to the designated person concerned.

Section III – The Court as controller and internal data protection roles

Article 9 Internal controllers

1. The Court, as controller, shall assign data protection responsibilities to its internal controllers, who shall act exclusively under the Court's control to carry out processing operations.

Article 10 Designated persons

1. Each internal controller shall designate one or more persons who shall be entrusted with data protection responsibilities and provide the internal controller with assurance that all processing operations involving personal data within their area(s) of responsibility comply with the Regulation.
2. The Appointing Authority may designate one or more persons who shall be entrusted with data protection responsibilities for processing activities that are transversal and concern several different departments at the Court.
3. A designated person cannot delegate their role to any other member of the Court's staff. However, the Court or the internal controller can designate a deputy designated person, who shall perform the tasks of the designated person in the absence of the latter.

4. A designated person shall be either a director, a principal manager, or another staff member with managerial duties. For processing operations under the responsibility of an ECA directorate whose work supports the Court's core activities, the designated person shall be the director of that directorate. For processing operations under the responsibility of a chamber, the designated person shall be the principal manager assigned to an ECA task by the chamber³.
5. Without prejudice to the provisions of the Regulation concerning the obligations of the Court, each designated person shall:
 - (i) request the advice of the DPO to establish the record of processing activities for which they are responsible. The designated persons shall submit the records to the DPO;
 - (ii) consult the DPO before acting in response to a request pursuant to Articles 17 to 24 of the Regulation for the exercise of the rights of a data subject⁴;
 - (iii) implement technical and organisational measures to adequately protect data subjects and comply with the Regulation; they may seek the advice of the DPO in selecting these measures;
 - (iv) notify, involve and consult the DPO as of the earliest planning phase of any processing activity for which they are responsible, and of any new decision or project, internal policies, rules and procedures involving personal data protection;
 - (v) perform an assessment of risks for the rights and freedoms of data subjects. If the conditions of Article 39 of the Regulation apply, this assessment shall take the form of a DPIA;
 - (vi) inform the DPO about direct interactions between them and the EDPS in its supervisory capacity regarding the internal application of the Regulation;
 - (vii) seek the advice of the DPO when planning to restrict data subjects' rights⁵ in relation to processing activities for which they are responsible.

Article 11 Data protection coordinators

1. Each internal controller shall appoint at least one DPC.
2. The DPC should participate in the network of DPCs of the Court to ensure consistent implementation and interpretation of the Regulation, and to discuss subjects of common interest.
3. The DPC role may be combined with other roles. The Court or the internal controller shall ensure that any other roles are compatible with the DPC role.

³ Task means carrying out audits, providing reviews and delivering opinions.

⁴ See [this overview](#) of data subject rights for more details.

⁵ On the basis of ECA Decision 42-2021 adopting internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the European Court of Auditors or any subsequent decision replacing Decision No 42-2021.

Section IV – Final provisions

Article 12 Entry into force

1. This Decision shall enter into force on the day following its adoption.
2. Decision No 40-2021 adopting implementing rules concerning the Data Protection Officer pursuant to Article 45(3) of Regulation (EU) 2018/1725 is hereby repealed.
3. After entry into force, this Decision shall be published on the Court's website.

Done at Luxembourg, 12 February 2024

For the Court of Auditors

Tony Murphy
President