EUROPEAN
COURT
OF AUDITORS

Decision No 40-2021 adopting implementing rules concerning the Data Protection Officer pursuant to Article 45(3) of Regulation (EU) 2018/1725

THE 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 Decision No 11/2012 adopting implementing rules concerning the Data Protection Officer pursuant to Article 24(8) of Regulation (EC) No 45/2001;

HAVING REGARD TO the discussions held by the Court of Auditors at its meeting of 20 May 2021;

WHEREAS Regulation (EU) 2018/1725 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 (the "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;

HAS DECIDED:

Article 1 Definitions

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

1. "Responsible staff", means the person responsible on behalf of the Court for data processing operations carried out in fulfilment of the mission of the institution;
2. "Informant" means an individual who brings 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.

Article 2 Scope

This decision further defines the rules concerning the DPO pursuant to Article 45(3) of the Regulation. It shall apply to all activities in relation to the processing of personal data by or on behalf of the Court which are covered by the Regulation.

Article 3 Designation, Status and Independence

1. The Court shall designate the DPO from amongst persons who are staff members of the Court and who possess the necessary professional qualifications to be able to fulfil the tasks and duties referred to in Article 5 of this Decision. In addition to possessing expertise in data protection law and practices and adequate knowledge of the organisation, structure and functioning of the Court, the DPO shall demonstrate personal qualities such as integrity and a high standard of professional ethics.
2. The term of office of the DPO shall be five years, renewable for further periods of five years.

   For administrative purposes, he shall be attached to the Secretariat-General. In this context, the DPO shall participate in preparing the Annual Work Plan and the draft Preliminary Budget of the Secretary-General.
3. The DPO shall directly report to the Secretary-General.
4. The appointment of the DPO shall be communicated officially to all staff to ensure that his or her function is known within the Court. The Secretary-General shall publish the name and the contact details of the DPO internally on the Court's intranet, internal telephone directory and organisational charts. The DPO's functional e-mail address shall be included in the information to be provided by the responsible staff to data subjects when their data are collected. The Secretary-General shall register the DPO with the European Data Protection Supervisor ("EDPS").
5. The DPO may be dismissed with the consent of 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.
6. The Court shall ensure that the DPO is involved, properly and as early as possible, in all issues relating to the processing of personal data. The DPO therefore needs to be informed at the earliest planning phase, by the responsible staff, of any new decision or project that has data protection consequences.
7. 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:

   (a) 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, etc.;

   (b) ensuring that the DPO maintains expert knowledge and has access to continuous relevant training on data protection and other forms of professional development, including participation in the meetings of the DPO network.
8. The DPO shall publish an annual activity report that shall be taken into account in the context of the annual performance appraisal of the DPO, for which the Secretary-General shall ensure equal and fair treatment.

9. The DPO shall not suffer any prejudice because of the performance of his or her duties

10. The DPO shall act in an independent manner with regard to the internal application of the provisions of the Regulation and shall not be instructed regarding the exercise of his or her tasks.

Article 4 Conflicts of interest

1. The DPO may fulfil other tasks and duties, provided that they do not result in a conflict of interest. The Secretary-General shall ensure that other tasks and duties assigned to the DPO do not result in such 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 his or her 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 based on risk assessment and accountability. The DPO shall ensure that the responsible staff, 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 with the Regulation, with other applicable Union law containing data protection provisions and with the policies of the responsible staff or processor in relation to the protection of personal data. As part of these monitoring duties, the DPO may, in particular:

   (a) collect information to identify processing activities;

   (b) analyse and check the compliance of processing activities;

   (c) inform, advise and issue recommendations to the responsible staff or the processor;

   (d) carry out inspections and audits.

3. Responsible staff shall assist the DPO in the performance of the DPO's duties and provide the information which the DPO requests within 15 working days. The DPO shall assist the responsible staff in the preparation of their records of processing activities.

4. Pursuant to Article 31(5) of the Regulation, and building on the records provided by the responsible staff, 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 responsible staff to assess the data protection risks of the processing activities under their responsibility. The DPO shall provide advice and assist the responsible staff when carrying out a data protection impact assessment ("DPIA") pursuant to Article 39 of the Regulation. The DPO shall monitor its performance and consult the EDPS in case of doubt as to the need of a 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 informant 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 responsible staff as regards 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. Within the sphere of his or her competence, the DPO shall cooperate with the EDPS at the latter's request or on his or her own initiative.

11. The DPO shall ensure that the responsible staff inform data subjects of their rights and obligations pursuant to the Regulation in the context of processing activities. The DPO shall support the responsible staff in ensuring that the rights and freedoms of data subjects are not adversely affected by processing operations.

12. The DPO may make practical recommendations and give advice to the responsible staff and the processor for improvement of data protection within the Court and advise them on matters concerning the interpretation and application of the Regulation.

13. The DPO may, on his or her own initiative or at the request of the responsible staff or the processor, the Court's staff committee or any individual, investigate matters and occurrences directly relating to his or her tasks, and report back to the person who commissioned the investigation or to the responsible staff or the processor, in accordance with the procedure described in Article 8 of this Decision.

14. 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 enquiries or complaints. This inventory shall serve as a performance indicator to measure compliance with the Regulation. Enquiries pursuant to Articles 17 to 24 of the Regulation may not remain anonymous.

15. The DPO shall represent the Court on any internal matter relating to data protection. The DPO shall in particular attend meetings of interinstitutional committees and bodies or relevant bodies at international level.

16. For processing operations on personal data under his or her responsibility, the DPO shall act as the responsible staff.

17. In addition to the general tasks, the DPO shall:

    (a) submit an annual activity report to the Secretary-General, who shall forward it to the Administrative Committee and the Court for information;

    (b) cooperate with the DPOs of other EU institutions and bodies in carrying out their functions, in particular by exchanging experiences and best practices. The DPO shall participate in the dedicated network(s) of DPOs. The DPO is also encouraged to be part of other DPO networks;

    (c) when possible, exchange experience and practices with DPOs from other organisations;

(d) cooperate with the internal auditor of the Court, in particular to obtain assurance of compliance with the Regulation;

(e) be consulted in the elaboration of internal policies, rules and procedures related to processing operations on personal data;

(f) be consulted by the responsible staff on the draft contractual data protection terms for contracts with external service providers;

(g) be consulted before deciding whether a document requested should be released pursuant to Decision No 12-2005 regarding public access to Court documents;

(h) contribute to the Court's Annual Activity Plan and Activity Report.

18. 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 his or her DPO tasks and duties and without prejudice to the powers conferred by the Regulation, the DPO:

(a) may request legal guidance from the Legal Service;

(b) may, in the event of disagreement with the responsible staff or processor on the interpretation or implementation of the Regulation, inform the President or the Secretary-General (depending on who is responsible as Appointing Authority) before referring the matter to the EDPS;

(c) may perform investigations on request, or upon the DPO's own initiative, into matters and occurrences directly relating to the DPO's activities, applying the appropriate principles for inquiries and audits at the Court and the procedure described in Article 8 of this Decision;

(d) 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;

(e) shall be responsible for initial decisions on requests for access to documents held by the DPO under Decision No 12/2005 regarding public access to Court documents.

2. When making recommendations and rendering advice, the DPO may:

(a) call upon the responsible staff or the processor to comply with the data subject's request for the exercise of his or her rights pursuant to the Regulation;

(b) issue warnings to the responsible staff and processor when a processing operation infringes provisions of the Regulation, and call upon them to bring processing operations into compliance, where appropriate, in a specified manner and within a specified period;

(c) call upon the responsible staff or the processor to suspend data flows to a recipient in a Member State, to a third country or an international organisation;

(d) request the responsible staff or the processor to report within a set deadline to the DPO on the follow-up given to the DPO's recommendation or advice;

(e) bring to the attention of the Secretary-General or the President[1] a member of the responsible staff or a processor, in order to comply with the obligations under the Regulation and this Decision;

(f) in exercising his or her powers, the DPO will take account of the guidelines issued by the EDPS in the different fields.

Article 7 Consultation and complaints

1. The DPO may be consulted by the responsible staff and the processor, by the Staff Committee and by any individual on any matter concerning the interpretation or application of the Regulation. No one shall suffer prejudice on account of a matter brought to the attention of the DPO alleging that a breach of the Regulation has occurred.
2. Data subjects may contact the DPO with regard to all issues related to the processing of their personal data and to the exercise of their rights.
3. A person who has questions or complaints concerning data protection at the Court should in the first instance address these to the DPO, without prejudice to their right to contact the EDPS directly. The DPO may launch an investigation as described in Article 8 of this Decision upon such a question or complaint.

Article 8 Investigation procedure

1. The requests for an investigation mentioned in Article 5(13) of this Decision shall be addressed 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 is to be treated as confidential. In the event of manifest abuse of the right to request an investigation, for example where it is repetitive, abusive and/or pointless, the DPO shall inform the requestor that the request is not being pursued and give account of the reasons and shall not be obliged to report anymore to the applicant.
2. If the requestor is a data subject asking for an investigation into the processing of their personal data, or if the requestor 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 his or her unambiguous consent for the request to be handled otherwise.
3. The DPO shall request a written statement on the matter from the responsible staff for the data processing activity in question. The responsible staff shall provide a response to the DPO within 10 working days. The DPO may request complementary information from the responsible staff and/or from other parties within 10 working days.
4. 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.

[1] Depending on who the Appointing Authority is for the person concerned, either the President or the Secretary-General is to be informed.

Article 9 Responsible staff

1. Responsible staff shall ensure that all processing operations involving personal data within their area(s) of responsibility comply with the Regulation.
2. Responsible staff cannot delegate their role to any other Court staff member, legal person, public authority, agency or other body.
3. Without prejudice to the provisions of the Regulation concerning their obligations, responsible staff shall:
   (a) consult the DPO before acting in reply to a request pursuant to Articles 17 to 24 of the Regulation for the exercise of the rights of a data subject;
   (b) maintain a record of activities processing personal data under their responsibility and seek the advice of the DPO to establish the record. Responsible staff shall transmit the records to the DPO to create the register referred to in Article 31(5) of the Regulation;
   (c) notify and involve, as appropriate, the DPO as of the planning phase of any activity processing personal data;
   (d) perform an assessment of risks for the fundamental rights and freedoms of data subjects and document it in the record. If the conditions of Article 39 of the Regulation apply, this assessment shall take the form of a DPIA. They shall seek the advice of the DPO in performing this assessment;
   (e) implement, as an outcome of this assessment, technical and organisational measures to adequately protect data subjects and comply with the Regulation; they shall seek the advice of the DPO in selecting these measures;
   (f) seek the advice of the DPO if a prior consultation of the EDPS is needed, based on Article 40 of the Regulation;
   (g) inform the DPO about direct interactions between them and the EDPS in its supervisory capacity regarding the internal application of the relevant provisions of the Regulation.

Article 10 Processors

1. Contracts shall be concluded with external processors. Such contracts shall contain the specific requirements mentioned in Article 29(3) of the Regulation. Responsible staff shall consult the DPO on the draft contractual data protection terms.
2. Each processor shall maintain a record of all categories of processing activities carried out on behalf of the institution and shall communicate it to the institution upon request. The contract concluded with processors shall establish a duty, among others, to provide the institution with the necessary information to create the institution's records referred to in Article 31(1) of the Regulation.

Article 11 Joint responsible staff

Formal arrangements shall be concluded with joint responsible staff to allocate responsibilities for compliance with the Regulation. Responsible staff shall consult the DPO when drafting those arrangements.

Article 12 Audit on 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 on the processing of personal data in order 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).
3. The scope areas to be covered during the audit shall be defined by the DPO prior to the audit.
4. The audit shall include, but shall not be limited to, compliance with the requirements of the Regulation, with other applicable Union law containing data protection provisions and with the policies of the responsible staff or processor in relation to the protection of personal data. The audit may be focused on general issues such as determining 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 within the Court.
5. Before carrying out an audit, the DPO shall inform the responsible staff concerned who shall assist the DPO in the performance of this task and provide him or her with any relevant information within 20 working days.
6. The audit process shall provide an opportunity for the responsible staff concerned to respond to the observations and recommendations made by the DPO before the DPO finalises the audit findings.
7. Following completion of each audit, the DPO shall submit its findings to the responsible staff concerned and shall publish the executive summary on the Court's intranet.

Article 13 Register

1. The register mentioned in Article 5(4) of this Decision is a repository of the Court, which contains an extract from all the records (information referred to in Article 31(1)(a) to (g)) of activities processing personal data submitted by the responsible staff.
2. The register shall be accessible in an electronic version on the Court's premises. The electronic version shall also be published on the Court's website.
3. Any individual may submit a written request to the DPO for an extract of the register. The DPO shall reply within 10 working days.

Article 14 Cooperation with the EDPS

1. Within the area of his or her responsibility, the DPO shall respond to requests from the EDPS and cooperate at the latter's request or on his or her initiative, particularly as regards dealing with complaints and carrying out inspections.
2. The DPO shall inform the EDPS regarding any new development at the Court which has a bearing on the protection of personal data.

3. The DPO shall be informed of any interactions between the Court and the EDPS pursuant to the relevant provisions of the Regulation.

Article 15 Restrictions under Article 25 of the Regulation

The data subjects' rights provided for in Articles 14 to 20 of the Regulation, as well as in Articles 35 and 36 thereof, may be restricted based on Decision No xxx-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. Responsible staff shall seek the advice of the DPO when planning to apply these restrictions.

Article 16 Entry into force

1. This Decision shall enter into force on the day following its adoption.
2. Decision No 11-2012 adopting implementing rules concerning the Data Protection Officer pursuant to Article 24.8 of Regulation (EC) No 45/2001 is repealed.
3. After entry into force, this decision shall be published on the Court's website.

Done at Luxembourg, 20 May 2021

For the Court of Auditors

Klaus-Heiner Lehne
President