EIOPA-19/432
26 08 2019

Decision of the Executive Director adopting implementing rules concerning the Data Protection Officer pursuant to Article 45(3) of Regulation (EU) N° 2018/1725 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) N° 45/2001 and Decision N° 1247/2002/EC.

The Executive Director,

Having regard to the Regulation (EU) No 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 and bodies and on the free movement of such data[1], and in particular Article 45,

Having regard to the Regulation (EU) No 1094/2010 of the European Parliament and the Council of 24 November 2010 ("the EIOPA Regulation") establishing the European Supervisory Authority (European Insurance and Occupational Pensions Authority) ("EIOPA")[2], and in particular Article 53,

Whereas:

(1) Regulation (EU) No 2018/1725, hereinafter referred to as "the Regulation", sets out the principles and rules applicable to all Union institutions, bodies, offices and agencies and provides for the appointment by each institution and agency of a Data Protection Officer.

(2) Article 45(3) of the Regulation requires that further implementing rules concerning the Data Protection Officer shall be adopted by each Union institution or agency. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer.

HAS DECIDED AS FOLLOWS:

[1] OJ L 295, 21.11.2018, p. 39.
[2] OJ L 331, 15.12.2010, p. 48.

Article 1 - Definitions

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

(1) EIOPA's Data Controller is EIOPA's Executive Director.
(2) "Internal data controllers" means middle managers to whom the tasks and the duties of the Data Controller may be individually or jointly delegated by the Executive Director.
(3) "Responsible staff" shall mean staff responsible on behalf of EIOPA for activities processing personal data in EIOPA.

Article 2 – Scope

This Decision further defines the rules and procedures for the implementation of the function of Data Protection Officer (hereinafter referred to as the "DPO") of EIOPA 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 EIOPA.

Article 3 – Appointment, Status and Independence

1. The Executive Director shall appoint the DPO from amongst the staff of EIOPA. The DPO shall have expert knowledge of data protection law and practices as well as a sound knowledge of EIOPA's mandate, its structure, its administrative rules and procedures. EIOPA shall ensure that the DPO tasks do not result in a conflict of interests with any other official tasks and duties conferred to the DPO.

2. The term of office of the DPO shall be for a period of three up to five years by decision of the Executive Director. The DPO shall be eligible for reappointment.

3. The Executive Director shall register the DPO with the European Data Protection Supervisor (EDPS).

4. The DPO shall ensure in an independent manner the internal application of the provisions of the Regulation and shall not be instructed regarding the exercise of his/her other tasks.

5. Without prejudice to the provisions of the Regulation concerning his/her independence and obligations, the DPO shall report directly to the Executive Director.

6. This reporting obligation shall be taken into account in the context of the annual performance appraisal of the staff member appointed as DPO (in particular with regard to the specific DPO duties), for which the Executive Director shall ensure an equal and fair treatment.

7. The DPO shall not suffer any prejudice on the account of the performance of his/her duties.

8. In accordance with the Regulation, the DPO may be dismissed from the post of DPO only with the consent of the EDPS, if they no longer fulfil the conditions required for the performance of their duties or at the request of the DPO for reasons that do not compromise the exercise of his/her functions.

9. The DPO shall maintain, including once he/she has ceased his or her duties, professional secrecy as regards any confidential documents or information, which he/she obtains in the course of his/her duties.

Article 4 - Duties and Tasks

1. The DPO shall inform and advise EIOPA staff members on the personal data protection legislation in force, current procedures and existing records. He/she shall carry out his/her tasks in cooperation with the European Data Protection Supervisor.

2. The DPO may be consulted at any time by any person and in particular by data subjects in respect of any matter relating to the application of the Regulation.

3. The DPO shall represent EIOPA in respect of any internal matter relating to data protection. He/she may in particular attend meetings of committees or relevant bodies at international level.

4. The DPO's tasks shall be as follows:

   (a) *Assistance with regard to the recordings, impact assessments and prior consultation of the EDPS*: the DPO shall inform/advise EIOPA's staff who process personal data as part of their functions at EIOPA, on the application of the provisions laid down in the Regulation, and more in particular with regard to the drafting of the recording, Data Protection Impact Assessments and submissions for prior consultations of the European Data Protection Supervisor in line with Articles 31, 39 and Article 40 of the Regulation.

   (b) *Assistance in the notification of a personal data breach:* the DPO shall assist the Executive Director acting as controller in the notification of a personal data breach to the EDPS in accordance with Article 34 of the Regulation.

   (c) *Cooperation with the EDPS:* within his/her area of responsibility, the DPO shall cooperate with the European Supervisor at the latter's request or on his or her own initiative, particularly as regards dealing with complaints and carrying out inspections. The DPO shall inform the European Supervisor regarding any significant development at EIOPA, which has a bearing on the protection of personal data.

   (d) *Publication of a central register of records:* the DPO shall, pursuant to Article 31 of the Regulation, ensure that the central register of the records of processing activities maintained by the internal data controllers is publicly available.

(e) *Data subject rights:* the DPO shall ensure that responsible staff inform data subjects of their rights and obligations pursuant to the Regulation in the context of processing activities; the DPO shall ensure that processing operations do not undermine the rights and freedoms of data subjects without any legal basis for restricting those rights, and that no person suffers loss or damage for having brought to the DPO's attention a matter which in the view of that person constitutes an infringement of the Regulation. The DPO shall ensure that rights and obligations of data subject rights are easily accessible on EIOPA's public website or Incidernet.

(f) *Monitoring of compliance:* The DPO may decide to carry out any type of monitoring at any time in order to ensure that the Regulation is being properly applied by EIOPA. EIOPA staff members shall ensure full assistance to the DPO in the performance of his/her duties and provide him/her with any information which he/she requests within 20 working days.

Article 5 – Powers

1. In performing his/her tasks and duties of the DPO and without prejudice to the powers conferred by the Regulation, the DPO may:

   (a) on his/her own initiative, make recommendations to the Executive Director or to the internal data controllers on issues concerning the application of the provisions relating to data protection or included in these implementing rules, or for the concrete improvement of data protection;

   (b) investigate issues and facts (on his/her own initiative or at the request of the Executive Director, EIOPA's Staff Committee or any individual) which relate directly to his/her powers and responsibilities and which have been brought to his/her knowledge. He/she shall consider them in accordance with the principle of impartiality and with due regard to the rights of the data subject. The DPO shall forward his/her findings to the person who submitted the request and to the Executive Director or to the internal data controllers; report any breach of the provisions laid down in the Regulation to the Executive Director;

   (c) issue an opinion on the lawfulness of actual or proposed processing operations, on the measures required in order to ensure that such operations are lawful and on the suitability or inadequacy of data or of security measures, if necessary. The opinion may in particular relate to any issue concerning the notification of data-processing operations.

   (d) may bring to the attention of the Executive Director and the human resources service any failure by a staff member to comply with the obligations pursuant to the Regulation; and

   (e) may request an opinion from the relevant areas of EIOPA on any issue associated with his/her tasks and duties.

2. In performing his/her duties, the DPO shall have access at any time to data being processed, to all premises, all data processing installations, including those of processors, and all information media.

3. No-one shall suffer prejudice on account of bringing a matter to the DPO's attention alleging a breach of the provisions of the Regulation.

Article 6 – Resources

1. EIOPA shall provide the DPO with the necessary resources to carry out his/her tasks and duties.

2. The DPO may be assisted in his/her day-to-day activities by a DPO-assistant.

3. The DPO may delegate his/her tasks and be represented (in his/her absence or when otherwise engaged) by one or more deputies, as necessary. The provisions on independence in Article 3(4) of this Decision apply to the deputies

4. The DPO shall have access to the necessary training and the opportunity to maintain his/her knowledge up-to-date with regard to the legal aspects of data protection. This applies mutatis mutandis to the DPO-assistant and the deputies.

Article 7 - Information and cooperation

1. The DPO shall be consulted, as appropriate, with regard to internal projects directly relating to the internal application of the provisions of the Regulation, and informed about opinions concerning the interpretation or implementation of other legal acts related to the protection of personal data and access to personal data.

2. The DPO shall be involved properly and in a timely manner in all issues, which relate to data protection at EIOPA.

4. EIOPA staff shall cooperate with the DPO in the performance of his/her duties, in particular for the conduct of investigations referred to in Article 5, point 1 (b), without requiring further authorisation.

3. The DPO shall update the Executive Director by means of regular meetings.

4. The DPO shall cooperate closely with EIOPA's internal network of Data Protection Coordinators (DPCs), who have to be designated in every Department/ Unit or Team. The DPO shall meet the DPCs regularly to discuss relevant topics, EDPS Guidelines, law cases, and new EIOPA processing activities. The DPCs shall assist their respective Department/Unit/Team in informing the DPO of upcoming processing activities and breaches of personal data.

Article 8 - Staff responsible for activities processing personal data

1. Responsible staff shall ensure that all processing operations involving personal data within their area(s) of responsibility comply with the Regulation.

2. Without prejudice to the provisions of the Regulation concerning their obligations, responsible staff shall:

   (a) Maintain a record of activities processing personal data under their responsibility and seek advice to the DPO to establish the record. They will transmit the records to the DPO to complete the register as referred to in Article 31(5) of the Regulation;

   (b) Notify and involve, as appropriate, the DPO as of the planning phase of any activity processing personal data;

   (c) 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 Data Protection Impact Assessment. They shall seek the advice of the DPO in performing this assessment;

   (d) 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;

   (e) Seek the advice of the DPO in case a prior consultation of the EDPS is needed, based on Article 40 of the Regulation;

   (f) Inform the DPO and his/her line manager on a breach of personal data as soon as possible, also in view of a possible notification to the EDPS and/or data subject pursuant to Article 34 and 35 of the Regulation;

3. The Local Security Officer shall inform the responsible staff as well as the DPO in case of a personal data breach without undue delay, including when there is doubt on whether personal data are affected by the security breach. The Local Security Officer shall provide the DPO with all the necessary information enabling him/her to ensure that EIOPA complies with the Regulation and more specifically with the obligation on personal data breach notifications and communications of Articles 34 and 35 of the Regulation.

Article 9 – Processors

1. Formal contracts with external processors shall contain the specific requirements mentioned in Article 29(3) of the Regulation. Responsible staff shall consult the DPO on the draft data protection contractual terms.

2. Each processor shall maintain a record of all categories of processing activities carried out on behalf of EIOPA and shall communicate it to EIOPA upon

request. The contract with them shall establish a duty, among others, to provide EIOPA with the necessary information to create EIOPA's records referred to in Article 31(1) of the Regulation.

Article 10 - Joint controllers

In the exercise of its mandate, EIOPA may act as joint controller together with one or more controllers as set forth in Article 28 of the Regulation. The responsibilities of the joint controllers for compliance with data protection obligations may be established in Union law or by further legal instruments.

Article 11 – Central Register

1. The register mentioned in Article 4, point 4 (a) hereof is a repository of EIOPA that contains all the records of activities processing personal data submitted by the responsible staff.

2. This central register shall provide information to data subjects and facilitate the exercise of their rights in line with Articles 17 to 24 of the Regulation. The central register shall be shall be accessible in electronic format and contain at least the information referred to in Article 31(1)(a) to (g) of the Regulation.

3. The register containing a general description of the processing activities at EIOPA shall also be published on EIOPA's website.

Article 12 - Exercise of Rights by Data Subjects

When data subjects contact EIOPA to exercise their rights pursuant to Articles 17 to 24 of Regulation, the responsible staff shall consult the DPO before replying to the data subject's request.

Article 13 - Restrictions Article 25

The data subject rights provided by Articles 14 to 22 of the Regulation as well as by Articles 35 and 36, may be restricted based on EIOPA's internal rules under Article 25(1) (EIOPA-MB-19/056-Rev1). Responsible staff shall seek the advice of the DPO when planning to apply these restrictions.

Article 14 – Remedies

1. Any person employed by EIOPA may lodge a complaint in accordance with Chapter VIII of the Regulation.

2. If any person employed by EIOPA lodges with the Appointing Authority a complaint pursuant to Article 90 of the Staff Regulations in respect of a matter relating to the processing of personal data, the DPO may be consulted, where appropriate.

Article 15 – Final provisions

1. The Executive Director may adopt measures necessary for implementation of this Decision.

2. This Decision shall enter into force on the day of its adoption.

3. After entry into force, this Decision shall be published on the EIOPA website.

Done in Frankfurt on 26 August 2019

Fausto Parente

EIOPA, Executive Director