

## DECISION OF THE EUROPEAN DATA PROTECTION BOARD

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 EUROPEAN DATA PROTECTION BOARD

Having regard to Regulation (EU) No 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 (General Data Protection Regulation),<sup>1</sup>

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data<sup>2</sup>, and in particular Article 45(3),

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 body of a Data Protection Officer (hereinafter referred to as "DPO").

(2) Article 45(1), letters (a) to (h), and 45(2) of the Regulation, set out the tasks of the DPO.

(3) Article 44(6) indicates that the DPO may fulfil other tasks and duties, provided that they do not result in a conflict of interests.

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

HAS DECIDED AS FOLLOWS:

### **Article 1 ("Definitions")**

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

(1) "European Data Protection Board" (hereinafter referred to as "EDPB" or the "Board") shall mean the body defined in articles 68 to 76 of Regulation 2016/679 (hereinafter referred to as the "GDPR") and include its Secretariat;

---

<sup>1</sup> OJ L 119, 4.5.2016, p. 1–88.

<sup>2</sup> OJ L 295, 21.11.2018, p. 39.

(2) “members of the Board” shall mean members of the EEA data protection authorities that compose the Board, and the European Data Protection Supervisor;

(3) "responsible staff" shall mean staff of the Secretariat responsible, on behalf of the EDPB and its Secretariat, for the performance of activities of the Board that involve the processing of personal data;

(3) "DPO" shall mean the Data Protection Officer and the Assistant(s)/Deputy(s) Data Protection Officer, forming the Data Protection Office of the EDPB.

## **Article 2 (“Scope”)**

This Decision further defines the rules and procedures for the implementation of the function of DPO, and its Deputy(ies), of the Board, 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 Board.

## **Article 3 (“DPO designation, status and independence”)**

1. The DPO shall be designated based on his or her professional qualities. One or more Deputy DPO(s) may be designated in accordance with the same procedure, to support the DPO in all his or her duties, and to ensure the continuity of the function in his or her absence.

2. The term of office of the DPO shall be for a period of three up to five years by decision of the Director, after consulting with the Chair of the Board and the Head of the EDPB Secretariat. The DPO shall be eligible for reappointment.

3. In accordance with the Regulation, the DPO and the Deputy DPO may be dismissed from their respective positions only with the consent of the European Data Protection Supervisor (hereinafter “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 compromise the exercise of his or her functions.

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 or her other tasks. The EDPB 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.

5. The DPO shall be selected from the staff of the EDPB Secretariat and not be shared with other EU institutions, bodies, offices or agencies. The DPO must have expert knowledge of data protection law and practices, as well as a sound knowledge of the EDPB services, its structure, administrative rules and procedures.

6. Without prejudice to the provisions of the Regulation concerning his or her independence and obligations, the DPO shall report directly to the Head of the EDPB Secretariat and to the Chair of the EDPB. 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 Head of the EDPB Secretariat shall ensure an equal and fair treatment.

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

8. The DPO shall be involved properly, and in a timely manner, in any issues which relate to data protection and the processing of personal data at, and/or in the context of the activities of the EDPB.

#### **Article 4 (“Tasks and Duties”)**

1. Without prejudice to the tasks described in Article 45 of the Regulation, the DPO shall raise awareness on applicable data protection law and encourage a culture of protection of personal data and accountability within the services involved in the processing of personal data.

2. The DPO shall monitor the implementation of the Regulation in the EDPB and regularly inform the Head of the EDPB Secretariat and the Chair of the EDPB.

3. The DPO shall assist the EDPB, represented by its Chair in the preparation of the EDPB records of processing activities. In exceptional circumstances (e.g. urgent cases), the DPO may prepare the first draft on behalf of the Chair of the EDPB. In performing their duties, the DPO shall have access, at all times, to personal and non-personal data being processed in the context of a given processing operation. The DPO shall also have access to all offices, data-processing installations and data carriers, including those of processors.

4. The DPO shall liaise with the DPOs of EDPB members regarding any matters pertaining to common or joint processing operations or activities, in order to ensure compliance of all parties with applicable legislation.

5. 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 institution. Following consultation of the Head of the EDPB Secretariat and approval by the Chair of the EDPB, the Board shall make the register publicly accessible.

6. The DPO shall help the EDPB, represented by its Chair to assess the data protection risks of the processing activities under its responsibility. The DPO shall provide advice and assist the EDPB, represented by its Chair when carrying out a general risk assessment and a data protection impact assessment (hereinafter “DPIA”), pursuant to Article 39 of the Regulation. He or she shall monitor its performance and consult the EDPS in case of doubts as to the need for a DPIA. The DPO will also advise on what methodology to use, and contribute to the selection of risk-mitigating safeguards to the rights and freedoms of data subjects, as well as on the correct implementation of the DPIA.

7. The DPO shall assist the EDPB, represented by its Chair on the need for prior consultation of the EDPS, pursuant to Article 40 of the Regulation.

8. The DPO shall assist the EDPB, represented by its Chair, in replying to requests for data subject rights, pursuant to Articles 17 to 24 of the Regulation, as well as to any requests for

information concerning the processing of personal data in the context of the activities of the Board. The DPO may also act as responsible staff for managing said data subjects' requests and requests for information on behalf of the Board.

9. The DPO shall provide advice, where requested, to the EDPB, represented by its Chair, as regards the necessity for a notification or a communication of a personal data breach, pursuant respectively to Articles 34 and 35 of the Regulation.

10. The DPO shall ensure that the EDPB, represented by its Chair, informs data subjects of their rights and obligations pursuant to the Regulation in the context of processing activities. They shall support the EDPB, represented by its Chair, in ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the activities processing personal data.

11. The DPO may keep a confidential inventory of requests from individuals that wish to reveal their identity only to the DPO when lodging enquiries or complaints. Enquiries pursuant to Articles 17 to 24 of the Regulation may not remain anonymous.

12. The DPO may make recommendations and give advice to the members of the Board, to its Chair and to processors working on behalf of the Board, on matters concerning the application of the Regulation. They may perform investigations on request, or upon their own initiative, into matters and occurrences directly relating to their tasks, and report back to the person who commissioned the investigation or to the controller, in accordance with an internal procedure developed for such purpose. If the applicant is a data subject asking for an investigation on the processing of their personal data, or if the applicant acts on behalf of the data subject concerned, the DPO must, to the extent possible, ensure the confidentiality on the request, unless the data subject concerned gives his or her unambiguous consent for any necessary disclosure.

13. Without prejudice to the independence of the DPO, the Head of the EDPB Secretariat may ask the DPO to represent the EDPB on any issues relating to the internal application of the provisions of the Regulation, including participation in, or coordination of, any networks related to the DPO's tasks.

14. In addition to their tasks within the EDPB, the DPO shall cooperate with the DPOs of other institutions, bodies and, where possible, organisations, in carrying out their functions, with special regard to the EDPS DPO, in view of the EDPS-EDPB Memorandum of Understanding<sup>3</sup>, by exchanging experiences and best practices.

15. For processing operations on personal data under his or her responsibility outside of his role as a DPO, the DPO shall act as responsible staff.

## **Article 5 (“Powers”)**

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

---

<sup>3</sup> Available at: [https://edpb.europa.eu/about-edpb/board/rules-procedure-and-memorandum-understanding\\_en](https://edpb.europa.eu/about-edpb/board/rules-procedure-and-memorandum-understanding_en)

- (a) May request legal guidance from the Head of the EDPB Secretariat, the Chair of the EDPB or the members of the Board;
- (b) May, in the event of disagreement with the Chair of the EDPB on the interpretation or implementation of the Regulation, inform the Head of the EDPB Secretariat and request guidance from the members of the Board;
- (c) In case of an incident, may, after informing the relevant staff member(s), and suggesting safeguards to prevent future similar incidents, bring to the attention of the Head of the EDPB Secretariat and the Chair of the EDPB any failure of a staff member to comply with the obligations under the Regulation;
- (d) May investigate matters and occurrences directly relating to the tasks of the DPO, applying the appropriate principles and legal provisions pertaining to such audits, and the procedure described in Article 10 hereof;
- (e) Shall be given access to personal and non-personal data being processed in the context of a given processing operation, as well as to all offices, data-processing installations and data carriers, including those of processors;
- (f) Shall have the support and assistance of the EDPB IT team, including those provided to the Board by external organisations, and may request technical opinions from the Local Information Security Officer (hereinafter “LISO”);

2. In exercising his or her powers, the DPO will take account of the Guidelines issued by the EDPS and the EDPB in different fields.

3. Without prejudice to applicable confidentiality or security rules, every responsible staff and any other EDPB secretariat’s staff shall assist the DPO in performing his or her duties.

#### **Article 6 (“Resources”)**

The DPO shall be provided with the necessary resources to carry out his or her tasks and duties. The DPO shall have access to the necessary training and the opportunity to maintain his or her knowledge up-to-date with regard to the legal and technical aspects of data protection.

#### **Article 7 (“Information”)**

The DPO shall inform the Head of the EDPB Secretariat and the Chair of the EDPB by means of reports and dedicated meetings. The DPO shall submit to the Head of EDPB Secretariat and the Chair of the EDPB an annual overview on his or her activities and on the state of play as regards the data protection activities and compliance of the Board. Where relevant, the Chair of the EDPB may ask the DPO to share this overview with the members of the Board.

#### **Article 8 (“Responsible person for activities processing personal data”)**

1. The EDPB, represented by its Chair, 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, the EDPB, represented by its Chair shall:

- (a) maintain a record of activities involving the processing of personal data under their responsibility and seek advice from the DPO to establish said record. They will transmit the records to the DPO to create the register, as stipulated in Art. 31(5) of the Regulation;
- (b) notify and involve, as appropriate, the DPO in any activities or procedures involving the processing of personal data, as of the planning phase of any such activity;
- (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 DPIA. 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;

3. In case of a personal data breach, the LISO shall inform the responsible staff, as well as the DPO, without undue delay, including when there are doubts on whether personal data are affected by the security breach. The LISO shall provide the DPO with all the necessary information enabling them to ensure that the institution complies with the Regulation and, more specifically, with any obligations on personal data breach notifications and communications stemming from Articles 34 and 35.

#### **Article 9 (“Processors”)**

1. Formal contracts shall be concluded with external processors. Such contracts shall contain the specific requirements mentioned in Article 29(3) of the Regulation. The EDPB, represented by its Chair, shall consult the DPO on the draft data protection contractual terms. Where necessary, the EDPB DPO will liaise with the DPOs and Data Protection Coordinators of other EU institutions and bodies, with particular reference to the EDPS.

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 with them shall establish a duty, among others, to provide the institution with the necessary information to create the institution’s records referred to in Art. 31(1) of the Regulation.

#### **Article 10 (“Joint controllers”)**

Formal arrangements shall be concluded with joint controllers to allocate responsibilities for compliance with the Regulation, unless, and in so far as, such responsibilities have not been determined by Union or Member State law to which the joint controllers are subject. The EDPB, represented by its Chair, shall consult the DPO on those draft agreements.

#### **Article 11 (“Register”)**

1. The register mentioned in Article 4(5) hereof is a repository of the EDPB activities involving the processing of personal data, exception being made to any activities, which, due to the nature

of the relationship between the EDPS and the EDPB, remain the full responsibility of the EDPS. Such activities shall be detailed in the Memorandum of Understanding between both institutions.

2. The register shall be accessible in electronic format in the EDPB Secretariat premises. The electronic format of the register shall also be published on the EDPB website.

3. Any individual can request an extract of the register in writing to the DPO, who shall reply as soon as possible and, in any event, no longer than one month following the request.

### **Article 12 (“Restrictions to data subject rights”)**

Data subject rights may be restricted based on EDPB internal rules, pursuant to Art. 25(1) of the Regulation. The EDPB, represented by its Chair, shall seek the advice of the DPO when deciding on the need to develop or planning to apply such restrictions.

### **Article 13 (“Entry into Force”)**

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

2. After entry into force, this Decision shall be published on the EDPB website.

Adopted by the EDPB Plenary, in Brussels, on 20 October 2020.