2019-185 REV 1

Decision No 2019-185 REV 1 of 09.10.2019 of the Management Board of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (hereinafter 'eu-LISA')

Subject: **Decision of the Management Board of eu-LISA on implementing rules concerning the Data Protection Officer pursuant to Article 45(3) of Regulation (EU) No 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) No 45/2001 and Decision No 1247/2002/EC**

THE MANAGEMENT BOARD of eu-LISA,

Having regard to 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, 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[1], and in particular Article 45(3) thereof,

Having regard to the Position Paper of the European Data Protection Supervisor of 30 September 2018 on the role of Data Protection Officers of the EU institutions and bodies[2],

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.

(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 body. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer.

(3) Regulation (EU) No 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and

[1] OJ L 295, 21.11.2018, p.39.
[2] Available at the EDPS website, via https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf.

repealing Regulation (EU) No 1077/2011[3], hereinafter referred to as "eu-LISA Regulation", formally establishes eu-LISA and defines the legal status of the Agency, its tasks and its internal management structure.

(4) Article 35(2) of the eu-LISA Regulation requires the Management Board to adopt measures for the application of the Regulation by eu-LISA, including measures concerning the Data Protection Officer. It also requires those measures to be adopted after consulting the European Data Protection Supervisor ("EDPS").

(5) The EDPS was consulted on these internal implementing rules and delivered an opinion on 11 June 2019.

HAS DECIDED AS FOLLOWS:

Article 1

Definitions

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

(1) "Agency" shall mean the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (hereinafter referred to as "eu-LISA").

(2) "Data Controller" shall mean the Agency itself, which alone or jointly with other determines the purposes and means of the processing of personal data and is legally responsible for such processing operation.

(3) "Responsible staff" shall mean staff responsible on behalf of the Agency for activities processing personal data in the Agency. The Data Protection Officer, hereinafter referred to as "the DPO", shall act as responsible staff for processing operations on personal data under his or her responsibility.

Article 2

Scope

This Decision defines the rules and procedures for the implementation of the function of the DPO within the Agency, without prejudice to the Regulation and provisions on data protection laid down in the legislative instruments governing the development, establishment, operation and use of large-scale IT systems whose operational management has been entrusted to the Agency. It shall apply to all activities in relation to the processing of personal data by or on behalf of the Agency.

[3] OJ L 295, 21.11.2018, p. 99.

Article 3

Appointment, status and independence

1. The Management Board shall appoint the DPO. The Agency shall publish the contact details of the DPO and the Executive Director shall communicate them to the EDPS.

2. An Assistant DPO may be designated in accordance with the same procedure and for the same term, to support and assist the DPO in all his or her duties and to ensure the continuity of the function in his or her absence.

3. The DPO shall be designated for a term of three to five years. The DPO shall be eligible for reappointment.

4. The DPO shall be selected on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. Additionally, the DPO should have a sound knowledge of the Agency's administrative rules and procedures.

5. 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 tasks.

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

7. The DPO shall monitor compliance with the Regulation, with other applicable Union law containing data protection provisions and with the policies of eu-LISA in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits.

8. The DPO shall be involved properly and in a timely manner in all issues, which relate to the protection of personal data at the Agency.

9. The DPO tasks shall not result in a conflict of interest with any other official tasks and duties conferred to the DPO.

10. The DPO, the Assistant DPO and their staff shall be bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union law.

11. Without prejudice to the provisions of the Regulation concerning his or her independence and obligations, the DPO shall report to the Management Board in the performance of his or her duties as DPO.

12. In accordance with the Regulation, the DPO and the Assistant DPO may be dismissed from the post of DPO or Assistant 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.

Article 4

Tasks and duties

These are without prejudice to the tasks as described in Article 45 of the Regulation.

1. *Inform and raise awareness*: the DPO shall raise awareness on applicable data protection law and encourage a culture of protection of personal data and accountability within the Agency.

2. *Advise*: the DPO shall make recommendations and give advice to responsible staff on matters concerning the application of the Regulation, by:

    (a) supporting responsible staff in ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the activities processing personal data. In particular, 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 assist responsible staff in the preparation of their records of processing activities;

    (b) helping responsible staff to assess the data protection risks of the processing activities under their responsibility. The DPO shall provide advice and assist responsible staff when carrying out a Data Protection Impact Assessment 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 for a Data Protection Impact Assessment. The DPO shall also advise on what methodology to use and shall contribute to selecting safeguards to apply to mitigate the risks to the rights and freedoms of the data subjects, as well as to the correct implementation of the Data Protection Impact Assessment;

    (c) assisting responsible staff on the need for prior consultation of EDPS pursuant to Article 40 of the Regulation;

    (d) advising where requested 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;

    (e) being consulted by any individual, without going through the official channels, on any matter concerning the interpretation or application of the Regulation.

3. *Organisational function*: building on the records provided by the responsible staff, the DPO shall keep a register of the processing activities, a register of personal data breaches and a register on data transfers carried out by the Agency. The DPO shall make a version of the register of processing activities publicly accessible pursuant to Article 31(5) of the Regulation.

4. *Cooperate*: the DPO shall respond to requests from the EDPS and, within the sphere of his or her competence, cooperate and consult with the EDPS at the latter's request or on his or her own initiative. The DPO shall also cooperate in carrying out his or her functions with the DPOs of other institutions and bodies, in particular by exchanging experience and best practices and shall participate in the dedicated network(s) of DPOs.

5. *Monitor compliance*: the DPO shall monitor the implementation of the Regulation in the Agency and issue an annual report as described in Article 7(4) of this decision.

6. *Handle queries or complaints*: The DPO may perform investigations on request, or upon his or her own initiative, into matters and occurrences directly relating to his or her tasks, and report back to the person who commissioned the investigation or to the controller, in accordance with the procedure described in Article 13 of this decision.

7. The DPO shall act as the single contact point for the EDPS on issues relating to processing, including the prior consultation referred to in Article 40 of the Regulation, and to consult, where appropriate, with regard to any other matter.

Article 5

Powers

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

   (a) may request legal guidance from the EDPS;

   (b) may, in the event of disagreement with the responsible staff on the interpretation or implementation of the Regulation, inform the competent management level and the Executive Director, before referring the matter to the EDPS;

   (c) may, after informing the staff member and their manager and suggesting safeguards to prevent future similar incidents, bring to the attention of the Executive Director any failure of a staff member to comply with the obligations under the Regulation with a view to a possible disciplinary action as specified in Article 69 of the Regulation;

   (d) may investigate matters and occurrences, on his own initiative or at the request of the responsible staff, directly relating to the tasks of the DPO, applying the appropriate principles for inquiries and audits at the Agency and the procedure described in Article 13 of this decision;

   (e) shall be able to obtain access at any time to the data forming the subject matter of processing operations on personal data and to all offices, data processing installations and data carriers;

   (f) may, with the agreement of the Executive Director, represent the Agency on any issues relating to the application of the provisions of the Regulation, including participation in interinstitutional committees and bodies;

   (g) may participate in security meetings and steering committees whenever issues relating to the processing of personal data are in the agenda.

2. Without prejudice to applicable confidentiality or security rules, every responsible staff shall assist the DPO in performing his or her duties and give information in reply to questions.

Article 6

Resources

1. The Agency shall provide the DPO 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 expert knowledge up-to-date with regard to the legal and technical aspects of data protection.

2. In accordance with paragraph 1, the DPO shall be provided with an Assistant DPO and other staff necessary to carry out his or her tasks. They shall be subject exclusively to his or her direction.

3. Given the split of the Agency between the seat in Tallinn and the technical site in Strasbourg, the DPO shall be provided with adequate resources at both sites.

4. The guarantee of independence in Article 3 of this decision applies also to the Assistant DPO and other staff provided in support to the DPO tasks.

Article 7

Information and consultation

1. The DPO shall be consulted before the adoption of any document related to data protection.

2. Without prejudice to Article 4(7) of this decision, the DPO shall be informed of any correspondence with the EDPS, in particular, whenever responsible staff consult the EDPS under Articles 34 and 40 of the Regulation.

3. The DPO shall be informed when responsible staff receive any request or complaint related to data protection matters.

4. The DPO shall inform the Executive Director by means of reports and dedicated meetings. The DPO shall submit to the Agency's Management Board an annual report on his or her activities and on the state of play as regards the data protection activities and compliance of the Agency. For publicity, both of these reports could be published.

5. The DPO shall contribute to the Consolidated Annual Activity Report and the Single Programming Document of the Agency.

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 obligations under the Regulation, the responsible staff shall:

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

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

   (c) Perform under their responsibility a Data Protection Impact Assessment if conditions of Article 39 of the Regulation apply. They shall document it in the record and seek advice from 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 on direct interactions between them and the EDPS without prejudice to Article 4(7) of this decision.

Article 9

Personal Data Breach

1. In case of a personal data breach, the Security Officer shall inform the responsible staff and the DPO without undue delay, including when they have doubts on whether personal data are affected by the security breach.

2. The responsible staff shall maintain a record of personal data breaches under their responsibility and seek advice of the DPO to establish the record. They shall transmit the signed records to the DPO to create the register as referred to in Article 12 of this decision.

3. The Security Officer and/or the responsible staff shall provide the DPO with all the necessary information enabling him or her to perform a risk assessment and to ensure that the Agency complies with the Regulation, specifically with the obligation on personal data breach notifications and communications of Articles 34 and 35.

Article 10

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

Article 11

Joint Controllers

Formal arrangements shall be concluded with joint controllers to allocate responsibilities for compliance with the Regulation. Responsible staff shall consult the DPO on those draft agreements.

Article 12

Registers

1. The registers mentioned in Article 4(3) of this decision are a repository of the Agency, which contains all the records of activities processing personal data, personal data breaches, and personal data transfers, respectively submitted by the responsible staff.

2. The registers shall be accessible in electronic format in the Agency's premises. A version of those registers without sensitive information shall also be made public.

3. Any individual may request an extract of the registers in writing to the DPO, who shall reply within 15 working days.

Article 13

Investigation Procedure

1. The request for an investigation mentioned in Article 4(6) hereof shall be addressed to the DPO in writing. Within 15 days upon receipt, the DPO shall send an acknowledgement of receipt to the person who commissioned the investigation and verify whether the request is to be treated as confidential.

2. Unless clearly stated otherwise, the DPO shall ensure confidentiality by default and in all cases.

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 15 working days. The DPO may request complementary information from the

responsible staff and/or from other parties within 15 working days. If appropriate, the DPO may request guidance from on the issue from the relevant Head of Unit. The DPO shall be provided with the guidance within 20 working days.

4. The DPO shall report back to the person who requested the investigation no later than three months following its receipt.

5. In the event of manifest abuse of the right to request an investigation, the DPO may not process the request. In that case, the DPO shall inform the applicant that the request is not being pursued and give account of the reasons.

6. No one shall suffer prejudice on account of a matter brought to the attention of the DPO alleging a breach of the provisions of the Regulation.

Article 14

Exercise of Rights by Data Subjects

1. When data subjects contact the Agency to exercise their rights pursuant to Articles 17 to 24 of the Regulation:

   (a) The request shall be addressed to the responsible staff or to the DPO in writing. Within 15 days upon receipt, an acknowledgement of receipt shall be sent to the applicant;

   (b) The responsible staff shall consult the DPO before acting in reply to the data subject's request. The DPO may act as responsible staff for managing data subject's requests on behalf of the Agency;

   (c) These rights may only be exercised by the data subject or his or her duly authorised representative. Such persons may exercise any of these rights free of charge;

   (d) The responsible staff shall grant the request only if the applicant's identity and, if relevant, his or her entitlement to represent the data subject, have been appropriately verified. The request shall contain at least an indication of the right(s) to be exercised, the category of the data concerned, the applicant's signature and date of the request. Where appropriate, supporting documents and/or additional information relating to the request may be requested by the responsible staff;

   (e) The responsible staff shall report back to the applicant no later than three months following the receipt of the request.

   (f) In the event of manifest abuse of the exercise of the rights pursuant to Articles 17 to 24 of the Regulation, for example when it is repetitive and/or may involve disproportionate effort, the responsible staff may not process the request.

Article 15

Restrictions Article 25

The data subjects rights provided by Articles 14 to 22 of the Regulation as well as by Articles 35 and 36, may be restricted based on eu-LISA internal rules under Article 25(1). 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 of its adoption.

2. After the entry into force, this Decision shall be published on the eu-LISA website.

Done in Tallinn on 09.10.2019