European Union Agency for Network and Information Security

DECISION No MB/2019/2

OF THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

implementing rules concerning the tasks, duties and powers of the Data Protection Officer pursuant to article 45(3) of Regulation (EU) 2018/1725

THE MANAGEMENT BOARD OF ENISA,

Having regard to the Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (hereinafter "ENISA"), and in particular article 29(2) thereof,

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, and in particular article 45(3) thereof,

Whereas:

(1) Regulation (EU) 2018/1725, hereinafter referred to as the "Data Protection Regulation", lays down the data protection principles and rules applicable to all European Union institutions and bodies and provides for a Data Protection Officer (hereinafter "DPO") to be appointed by each European Union institution and body;

(2) Pursuant to article 45(3) of the Data Protection Regulation, each European Union institution and body must adopt further implementing rules concerning the DPO in accordance with the provisions of that Regulation. The implementing rules shall in particular concern the tasks, duties and powers of the DPO;

(3) According to article 31 of the Data Protection Regulation, all Union institutions and bodies have an obligation to maintain records of their processing activities. These records shall be kept in a central register. The register shall be made publicly accessible.

(4) The Decision of the ENISA Management Board on implementing rules relating to Regulation (EC) No 45/2001 of the European Parliament and of the Council 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and on the free movement of such data (as amended) dated 28 October 2014 (ENISA MB Decision No MB/2014/16) should be repealed.

(5) The Executive Board of ENISA has reviewed this decision.

HAS ADOPTED THIS DECISION:

Article 1
Definitions

Without prejudice to the definitions provided in article 3 of the Data Protection Regulation, the following definitions shall apply:

"Controller" shall mean ENISA (as represented by its Executive Director), which alone or jointly with others determines the purpose and means of the processing of personal data and is legally responsible for such processing activity.

"Staff responsible for data processing activities" shall mean the persons responsible in practice for internally managing a data processing activity at ENISA, as delegated by the Controller.

"Data subject" shall mean any identified or identifiable natural person whose personal data are processed by ENISA; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 2
Subject matter and scope

1. This Decision lays down specific rules and procedures for the implementation of the function of the DPO at ENISA pursuant to article 45(3) of the Data Protection Regulation. It shall apply to all activities in relation to the processing of personal data by or on behalf of ENISA.

2. This Decision also clarifies certain rules with regard to responsibilities of the Controller and staff responsible for data processing activities with regard to the function of the DPO.

Article 3
Appointment, status and independence of the Data Protection Officer

1. The Executive Director shall appoint the DPO pursuant to article 43 and in order to fulfil the tasks laid out in article 45 of the Data Protection Regulation and register him or her with the European Data Protection Supervisor (hereinafter "EDPS").

2. The Executive Director may also appoint Deputy DPO(s). The role of a deputy DPO will be to support the DPO in carrying out his or her tasks and deputise in the event of the DPO's absence. The provisions of this Decision shall also apply in their entirety to a Deputy DPO.

3. The term of office of the DPO shall be for a period of three to five years. This term may be renewed.

4. The DPO may be dismissed from his or her post only with the consent of the EDPS and only if he or she no longer fulfils the conditions required for the performance of his or her

duties. The EDPS shall be consulted in writing by the Controller and a copy will be sent to the DPO.

5. The DPO shall be a staff member of ENISA. He or she shall be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred in article 45 of the Data Protection Regulation and article 4 of this Decision. The DPO shall also have adequate knowledge of the organisation, structure and functioning of ENISA, in particular adequate understanding of ENISA's data processing activities.

6. The DPO shall act in an independent manner with regard to the internal application of the provisions of the Data Protection Regulation. The DPO shall refrain from any act that is incompatible with the nature of his or her duties.

7. The DPO may be consulted by the Controller, the staff responsible for data processing activities, the ENISA staff committee or any individual, without going through the official channels, on any matter concerning the interpretation or application of the Data Protection Regulation. No one should suffer prejudice on account of a matter brought to the attention of the DPO alleging a breach of that Regulation. The 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.

8. The DPO shall by bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union law.

9. The DPO shall have resources necessary to carry out his or her tasks and to maintain his or her knowledge.

10. Taking into consideration the nature and the number of data processing activities at ENISA, the DPO function may be carried out on a part time basis. In such case, the allocation of time to the DPO function should not be less than 50%, while ensuring that any other tasks or duties that the DPO fulfils do not result in a conflict of interest with the DPO tasks.

11. The DPO shall report directly to the ENISA's Executive Director.

Article 4
Tasks and duties of the Data Protection Officer

1. Without prejudice to the tasks described in article 45 of the Data Protection Regulation, the DPO shall:

a) Provide advice to the Controller and the staff responsible for data processing activities with regard to all matters related to the internal compliance with the Data Protection Regulation.

b) Advise where requested the Controller and the staff responsible for data processing activities in the conduction of data protection impact assessments, as well as the prior consultation with the EDPS pursuant to articles 39 and 40 respectively of the Data Protection Regulation.

c) Advise where requested the Controller and the staff responsible for data processing activities in responding to data subjects' requests pursuant to articles 17 to 24 of the Data Protection Regulation.

d) Advise where requested the Controller and the staff responsible for data processing activities in the handling of personal data breaches, in particular with regard to the assessment of the likelihood and severity of the risk to the rights and freedoms of data subjects, and to the notification or communication of a personal data breach pursuant to articles 34 and 35 of the Data Protection Regulation.

e) Act as the main point of contact of the Controller for the EDPS and co-operate with the EDPS 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 EDPS regarding any significant development at ENISA which has a bearing on the protection of personal data.

f) Keep the central register of records of processing activities maintained by the staff responsible for data processing activities, as provided for in Article 31 of the Data Protection Regulation, and provide advice for the staff responsible for data processing activities with regard to the maintenance of these records.

g) Provide advice to the data subjects with regard to the exercise of their rights pursuant to articles 17 to 24 of the Data Protection Regulation, as well as with regard to relevant restrictions of these rights pursuant to article 25 of that Regulation.

h) Encourage, support, and implement a sensible and sound data protection culture within ENISA and among its staff by organising regular awareness raising sessions (trainings) in data protection, in particular to new staff joining ENISA, and by promoting protection of personal data as a key aspect of data processing activities at ENISA.

i) Cooperate with the DPOs of other European Union institutions and bodies, in particular by exchanging experience and sharing know-how and representing ENISA in discussions relating to data protection issues. To this end, the DPO shall regularly attend meetings with the EDPS and/or the DPOs of other European Union institutions and bodies (DPOs network) with a view to exchange best practices and harmonize the application of the Data Protection Regulation across the Union institutions and bodies.

2. In the first quarter of each calendar year, the DPO shall submit an annual report to the Executive Director in relation to data protection issues addressed in the previous year.

3. In the last quarter of each calendar year, the DPO shall submit to the Executive Director a work plan for the forthcoming year.

Article 5
Powers of the Data Protection Officer

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

a) On his or her own initiative, make recommendations to the Controller and the staff responsible for data processing activities on issues concerning the application of the provisions relating to data protection at ENISA.

b) Issue opinions on the compliance of actual or proposed data processing activities at ENISA with the Data Protection Regulation.

c) Perform, on his/her own initiative or at the request of the Controller, the staff responsible for data processing activities, the ENISA staff committee or any individual, investigations directly relating to his or her tasks and which come to his or her notice and report back to the person who commissioned the investigation or to the Controller, in accordance with article 45(2) of the Data Protection Regulation. The procedure for the DPO's investigation will be delivered by a Decision of the ENISA's Executive Director (ED Decision).

d) Bring to the attention of the Executive Director any breach of the provisions laid down in the Data Protection Regulation and failure of a staff member to comply with the obligations under that Regulation.

2. The DPO shall have access at all times to the data forming the subject matter of processing operations on personal data and to all offices, data-processing installations and data storage devices.

3. The staff responsible for data processing activities and any member of ENISA's staff shall be required to assist the DPO in performing his or her duties, especially for the conduct of investigations referred to in point 1(c) above, without requiring further authorisation.

Article 6
Controller and staff responsible for data processing activities

1. The Controller will ensure that the DPO is involved properly and in a timely manner in all issues relating to the protection of personal data at ENISA.

2. Without prejudice to the responsibility of the Controller, the staff responsible for data processing activities shall ensure that all processing operations involving personal data within their area(s) of responsibility comply with the Data Protection Regulation. For that purpose, the staff responsible for data processing activities shall:

a) Inform the DPO when an issue arises that has data protection implications, especially in the event of a personal data breach. The DPO shall also be informed before the adoption of any opinion, document, internal policy or internal decision that may have impact on ENISA's data protection compliance.

b) Inform the DPO when a data subject exercises his or her rights vis-à-vis the Controller where the articles 17 to 24 of the Data Protection Regulation are specifically invoked.

c) Consult the DPO with regard to compliance with the Data Protection Regulation of any data processing activity in their area of responsibility. The DPO shall also be consulted in the planning phase of any new data processing activity or change in existing data processing activities.

d) Maintain the records of data processing activities in their area of responsibility pursuant to article 31 of the Data Protection Regulation and co-operate with the DPO in the maintenance of the central register of data processing activities, as laid out in article 7 of this Decision.

Article 7
Central register

1. The staff responsible for data processing activities shall submit their records of processing activities pursuant to article 31 of the Data Protection Regulation to a central register. The DPO shall keep and manage the central register.

2. The central register shall serve as a repository of the personal data processing activities conducted at ENISA. It shall provide information to data subjects and facilitate the exercise of their rights in line with articles 17 to 24 of the Data Protection Regulation. The central register shall be publicly accessible. The central register shall contain at least the information referred to in article 31(1)(a) to (g) of the Data Protection Regulation.

Article 8
Final provisions

1. The Executive Director may adopt measures necessary to implement this decision by way of an ED Decision, having regard to the procedures for the DPO's investigation and any guidelines issued by the EDPS.

2. This decision repeals the decision MB/2014/16 of the ENISA Management Board of 28 October 2014 adopting implementing rules of Regulation (EC) 45/2001.

Article 9
Entry into force

The present decision shall enter into force on the day following that of its adoption. It will be published on the Agency website.

Done by written procedure on 22.05.2019.

On behalf of the Management Board,

[signed]

Jean-Baptiste Demaison

Chair of the Management Board of ENISA