



**DECISION No MB/2014/16**

**OF THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR  
NETWORK AND INFORMATION SECURITY  
Adopting implementing rules of Regulation (EC) 45/2001**

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 (ENISA), and in particular Article 29 (2) thereof,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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, and in particular Article 24(8) thereof,

Whereas:

(1) Regulation (EC) No 45/2001, 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 (DPO) to be appointed by each European Union institution and body;

(2) Pursuant to Article 24(8) of the Data Protection Regulation, each European Union institution or body must adopt further implementing rules concerning the DPO in accordance with the provisions in the Annex to that Regulation,

(3) The DPO for the European Union Agency for Network and Information Security, hereinafter referred to as "ENISA", was appointed by the Executive Director Decision 02/2014 of 17 January 2014.

(4) The DPO shall aim to ensure that the rights and freedoms of data subjects are unlikely to be adversely affected by processing operations and should advise both the data subjects and the management of ENISA as to how to ensure the compliance with the Data Protection Regulation.

(5) It is necessary to define who exercises the tasks of the data controller and to establish a framework concerning the notifications of processing operations and the register therefor.

HAS ADOPTED THIS DECISION:

*Article 1*  
**Subject matter and scope**

1. This Decision lays down the general rules implementing the Data Protection Regulation as regards ENISA. In particular, it supplements the provisions of the Data Protection Regulation relating to the DPO's appointment and status, as well as to their tasks, duties and powers.
2. This Decision also clarifies the roles, tasks and duties of controllers and implements the rules pursuant to which data subjects may exercise their rights.

*Article 2*  
**Definitions**

For the purposes of this Decision the definitions of Article 2 of the Data Protection Regulation shall apply.

*Article 3*  
**Appointment, status and organisational matters**

1. The Executive Director shall:
  - a) Ensure that a DPO is always in place and appointed pursuant to the Article 24 of the Data Protection Regulation;
  - b) Set a term of office for a DPO for up to two years. This term may be renewed.
  - c) Register the DPO with the European Data Protection Supervisor (EDPS).
2. The Executive Director may appoint a Deputy DPO. The Deputy DPO shall support the DPO in carrying out DPO tasks and duties and deputise in the event of the DPO's absence. The provisions of this decision shall also apply to the Deputy DPO in their entirety.
3. Given the load of data process in the Agency, the DPO functions shall be carried out in a part time manner.

*Article 4*  
**Data Protection Officer's tasks and duties**

1. The main tasks of the DPO are listed in the Article 24 of the Data Protection Regulation and in the Annex to that Regulation.
2. In addition, the DPO shall have the following tasks, duties and powers:
  - a) The DPO shall be the main point of contact for the EDPS and will support the Executive Director in this matter when he is addressed directly by EPDS;
  - b) Cooperate with the DPOs of other European Union institutions and bodies, in particular by exchanging experience and sharing know-how and representing ENISA in all discussions relating to data protection issues;

- c) 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.
  - d) In the last quarter of each calendar year, the DPO shall submit to the Executive Director a work plan for the forthcoming year.
3. In the daily performance of the tasks specified in Article 24 of the Data Protection Regulation and the Annex to that Regulation the DPO shall:
- (a) encourage, support and implement a sensible and sound data protection culture within ENISA and its staff;
  - (b) keep and maintain a register of processing operations provided for in Article 26 of the Data Protection Regulation. Data subjects may make use of the information contained in the register to exercise their rights under Articles 13 to 19 the Data Protection Regulation.

*Article 5*  
**The Data controller**

1. ENISA shall be the controller (hereinafter referred to as "Controller") as defined in the Article 2(d) of the Data Protection Regulation and referred to in Article 25 (2)(a) thereof.
2. The tasks of the controller are in practice exercised by the different units of the Agency. Accordingly, each Head of Unit shall be responsible for exercising the tasks of controller for the processes in his/her Unit (hereinafter referred to as "Delegated Controller").
3. The Delegated Controller shall give prior notice to the DPO of the information listed in the Article 25 (2) of the Data Protection Regulation on any processing operation in his/her Unit involving personal data.
4. When personal data is collected, the Delegated Controller shall provide a data subject with information, as defined in Article 11 and 12 of the Data Protection Regulation.
5. The Delegated Controller is responsible for the implementation of the Data Protection Regulation in his/her Unit and thus for ensuring that his/her staff have necessary procedures in place. The DPO shall assist the Delegated Controller in this function.

*Article 6*  
**Processing of personal data on behalf of controllers**

When the processing of personal data is delegated to a processor (which includes third parties, the Delegated Controller shall take appropriate measures to ensure a compliance with the Data Protection Regulation.

*Article 7*  
**Notification procedure**

1. Before introducing new processing operations relating to personal data, the relevant controller shall notify the DPO. Any processing operation that is subject to "prior checking" as defined in the Article 27 of the Data Protection Regulation shall be notified in advance of introduction to allow for "prior checking" by the EDPS.
2. The controllers shall immediately inform the DPO of any change affecting the information contained in a notification already submitted to the DPO.

*Article 8*  
**Final provisions**

1. The Executive Director is empowered to introduce procedures to give effect to the present decision and the requirements of the Data Protection Regulation.
2. This decision repeals the ED decision 04/2011 of 14 March 2011 Adopting implementing rules of Regulation (EC) 45/2001 at the European Network and Information Security Agency (ENISA).

*Article 9*  
**Entry into force**

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

Done at Vienna on 28 October 2014.

On behalf of the Management Board



*Chairperson*