EUDA
EUROPEAN UNION DRUGS AGENCY

DEC/MB/24/29

Decision of the Management Board of the European Union Drugs Agency (EUDA) establishing measures for the application of Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of individuals with regard to processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, including measures concerning the appointment of the Agency's data protection officer

THE MANAGEMENT BOARD,

Having regard to Regulation (EU) No 2023/1322 of the European Parliament and of the Council of 27 June 2023 on the European Union Drugs Agency (EUDA), in particular Article 47 (3) thereof,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and in particular Article 45(3) thereof,

After consulting the European Data Protection Supervisor (EDPS),

Whereas:

1. Regulation (EU) 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 Union institution, body, office, or agency of the 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 in accordance with the provisions in the Annex thereto. The implementing rules shall in particular concern the tasks, duties, and powers of the Data Protection Officer (DPO).
3. The implementing rules also specify the procedures for the exercise of rights of the data subjects, as well as for the fulfilment of obligations of all relevant actors within the Union institutions or bodies relating to the processing of personal data.
4. The implementing rules of the Regulation are without prejudice to Regulation (EU) 2018/1725.

HAS DECIDED AS FOLLOWS:

SECTION 1
GENERAL PROVISIONS

Article 1
Subject matter and scope

1. This decision lays down the general rules implementing Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. In particular, it supplements the provisions in Regulation (EU) 2018/1725 relating to the DPO's appointment and status, as well as to his/her tasks, duties, and powers.

2. Furthermore, the decision lays down the rules pursuant to which data subjects may exercise their rights and the procedure for notifying a processing operation to the Data Protection Officer.

Article 2

Definitions

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

a. 'Controller' shall mean the EUDA represented by its Executive Director, who may delegate her/his tasks to the Heads of the Unit to reflect the operational responsibilities, in line with Article 3(8) of the Regulation.

b. 'Agency staff' shall mean all permanent officials, temporary agents, contractual agents, and interim staff employed by the agency.

c. 'Data Subject' shall mean an identified or identifiable natural person who is the subject of the data.

SECTION 2
THE DATA PROTECTION OFFICER

Article 3

Appointment and status and organisational matters

1. The Executive Director of the EUDA appoints the DPO from amongst EUDA staff on the basis of his/her personal and professional qualities and in particular, his or her expert knowledge of data protection. The Executive Director registers him/her with the European Data Protection Supervisor (hereafter referred to as 'EDPS'). The DPO is directly attached, and reports, to the Executive Director. This reporting obligation shall be taken into account for the annual performance appraisal of the DPO for the specific DPO duties, for which the Executive Director shall ensure an equal and fair treatment. The term of office of the DPO shall be three years and is renewable up to a maximum total period of nine years.
2. With respect to the performance of his/her duties, the DPO shall act in an independent manner and in cooperation with the EDPS. In particular, the DPO shall not be instructed by the Executive Director nor from anyone else regarding the exercise of his/her duties, the internal application of the provisions of the Regulation or his/her cooperation with the EDPS.
3. The DPO may be dismissed from his/her function, only with the consent of the EDPS, if he/she no longer fulfils the conditions required for the performance of his/her duties.
4. Without prejudice to the procedure for his/her appointment, the DPO shall be informed of all contacts with external parties relating to the application of the Regulation, notably with regard to interaction with the EDPS.
5. Without prejudice to the relevant provisions of Regulation (EU) 2018/1725, the DPO and his/her staff shall be subject to the rules and regulations applicable to officials and other servants of the European Union.
6. The designation of the DPO shall be communicated officially to all EUDA staff, upon his or her appointment.
7. The DPO shall be provided with adequate resources necessary to carry out his or her duties, and 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.

8. The Executive Director ensures that the DPO tasks do not result in a conflict of interest with any other tasks and duties of the DPO.

Article 4

Data Protection Officer's tasks

The DPO shall:

1. ensure that controller is informed of their rights and obligations pursuant to the Regulation, and that the controller informs data subjects of their rights and obligations pursuant to the Regulation in the context of the EUDA processing activities. The DPO shall support the controller in ensuring that the rights and freedoms of the data subjects are not adversely affected by the activities requiring the processing of personal data. In the performance of this task, he/she shall in particular establish information and notification forms, consult interested parties and raise general awareness of data protection issues.
2. respond to requests from the EDPS and, within the sphere of his/her competence, cooperate with the EDPS at the latter's request or on his/her own initiative.
3. ensure in an independent manner the internal application of the provisions of the Regulation at the EUDA.
4. provide advice, upon request of the controller, on the correct implementation of the Data Protection Impact Assessment (DPIA) in relation to processing operations likely to present a high risk referred to in Article 39(1) of the Regulation, monitor its performance and consult the EDPS in case of doubt as to the need for a DPIA. The DPO shall in particular:

   - provide support to responsible staff to assess the data protection risks relating to the processing activities under their responsibility;

   - advise staff members on what methodology to use on a case-by-case basis; and,

   - advise on the selection of necessary safeguards to mitigate the risks to the rights and freedoms of data subjects.

Article 5

Data Protection Officer's duties

1. In addition to the general tasks to be fulfilled, the DPO shall:

   a. Act as an advisor to the controller on matters concerning the application of data protection provisions. The DPO may be consulted by the controller, the Staff Committee and by any individual, without going through the official channels, on any matter concerning the interpretation or application of the Regulation;

   b. On his/her own initiative or the initiative of the controller, the Staff Committee or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his/her notice, and report back to the Executive Director or the person who commissioned the investigation. If deemed appropriate, all other parties concerned should be informed accordingly. If the complainant is an individual, or in case the complainant acts on the behalf of an individual, the DPO must, to the extent possible, ensure confidentiality of the request, unless the data subject concerned gives his/her unambiguous consent to treat the request otherwise. The Staff Committee and all EUDA services must cooperate closely with the DPO in cases of an alleged breach of data protection rules, and ensure that he or she is duly informed and consulted;

   c. Cooperate with the Data Protection Officers of other Union institutions, bodies, offices, and agencies, in particular by exchanging experience and best practices, including participating in the dedicated network of EUI DPOs;

d. Represent the EUDA in all data protection related issues; without prejudice to his/her other duties, this may include the DPO's participation in relevant committees or forums at international level;

e. Submit an annual report on his/her activities to the Executive Director of the EUDA and make it available to the staff.

2. Without prejudice to the relevant provisions of the Regulation, the DPO and his/her staff shall not divulge information or documents which they obtain in the course of their duties.
3. The DPO shall be informed, as appropriate, about opinions and position papers of the EDPS directly relating to the internal application of the provisions of the Regulation, as well as about opinions concerning the interpretation or implementation of other legal acts related to the protection of, and access to, personal data.

Article 6

Data Protection Officer's powers

In performing his or her tasks and duties the DPO:

1. Shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations, including the carriers of the processors;
2. May request legal opinions from the legal advisor of the EUDA or ask the Executive Director to obtain an opinion from the European Commission;
3. May call on the services of external experts in information technologies upon prior agreement of the authorising officer in accordance with the Financial Regulation and its implementing rules;
4. May without prejudice to the EDPS' duties and powers, propose EUDA administrative measures and issue general recommendations on the appropriate application of the Regulation;
5. May make, in specific cases, any other recommendation for the practical improvement of data protection to the EUDA and/or to all other parties concerned;
6. May bring to the attention of the Executive Director of the EUDA any failure of a staff member to comply with the obligations under the Regulation and suggest an administrative investigation being launched in view of the possible application of Article 66 of the Regulation. The Executive Director may be notified after the DPO informed the concerned staff member(s) and his/her/their Head of Unit and suggest them safeguards to prevent similar future incidents.

SECTION 3

THE CONTROLLER

Article 7

Tasks and duties of the controller

1. The controller is responsible for ensuring that all processing operations under their control comply with the Regulation.
2. In particular, the controller shall:

a. Give prior notice to the DPO of any processing operation or set of such operations intended to serve a single purpose or several related purposes, as well as of any substantial change of existing processing operations. For processing operations carried out prior to the entry into force of the implementing rules, the controller shall notify without delay the DPO;

b. Assist the DPO and the EDPS in performing their respective duties, in particular providing information in reply to their requests within a reasonable period, depending on the circumstances of the case, and in any event, no later than thirty days;

c. Implement appropriate technical and organisational measures and give adequate instructions to EUDA staff to ensure both the confidentiality of the processing and a level of security appropriate to the risks represented by the processing;

d. Where appropriate, consult the DPO on the conformity of processing operations with the Regulation, and in particular when they have reason to believe that certain processing operations are incompatible with Articles 4 to 10 of the Regulation.

Article 8

Notification procedure

1. The controller shall notify to the DPO any processing operation of personal data on the basis of a notification form made accessible on the Data Protection pages on the EUDA's Intranet.
2. The notification shall include all information specified in Article 31 of the Regulation. Any change affecting this information shall be notified promptly to the DPO.
3. Further rules and procedures regarding the notification procedure to be followed by the controller shall form part of the general recommendations issued by the DPO.

SECTION 4

DATA SUBJECTS' RIGHTS

Article 9

Central Register

1. The DPO shall keep a central register of records of processing operations performed upon personal data, which shall be set up on the basis of the records provided by the controller of these operations.
2. The central register of records shall contain at least the information referred to in Article 31 of the Regulation.
3. Data subjects may make use of the information contained in the central register and facilitate the exercise of their rights set out in Articles 14 to 24 of the Regulation, in particular the right of access, rectification, blocking, erasure, and objection in relation to personal data.

Article 10

Exercise of data subjects' rights

Further to the data subject's right to be appropriately informed about any processing of their personal data, data subjects may approach the relevant controller to exercise their rights according to Articles 14 to 24 of the Regulation, as specified below:

1. The data subjects' rights may only be exercised by the individuals concerned or, in exceptional cases, on behalf of these individuals with proper authorization.
2. Requests shall be addressed in writing to the controller concerned with a copy to the DPO. If necessary, the DPO shall assist the data subject in identifying the controller concerned.

   The controller shall grant the request only if the complainant's identity has been verified properly. The exercise by data subjects of their rights shall be free of charge. The controller shall without delay

inform the data subject in writing of whether or not the request has been accepted. If the request has been rejected, the controller shall include the grounds for the rejection.

3. The controller shall at any time within one month of receipt of the request, grant access pursuant to Article 17 of the Regulation by enabling the data subject to consult these data on-site or to receive a copy thereof, according to the applicant's preference.
4. Data subjects may contact the DPO in the event the controller does not respect either of the time limits in paragraphs 2 or 3 above. In the event of obvious abuse by a data subject in exercising his/her rights, the controller may refer the data subject to the DPO. If the case is referred to the DPO, he/she will decide on the merits of the request and the appropriate follow-up. In the event of disagreement between the data subject and the controller, both parties shall have the right to consult the DPO.
5. Without prejudice to any judicial remedy, every data subject may lodge a complaint with the EDPS if he/she considers that his/her rights under the Regulation have been infringed as a result of the processing of his/her personal data by the EUDA. EUDA staff members may consult the DPO before lodging a complaint with the EDPS pursuant to Article 67 of the Regulation.
6. The exemptions and restrictions, as specified in Article 25 of Regulation (EU) 2018/1725, apply.

Article 11

Procedure for handling data breaches

In case of a personal data breach, the Security Officer shall inform the responsible staff as well as DPO without undue delay, including when they have doubts on whether personal data are affected by the security breach. The Security Officer shall provide the DPO with all the necessary information enabling him or her to ensure that the institution comply with the Regulation and more specifically with the obligation on personal data breach notifications and communications of Articles 34 and 35.

Article 12

Investigation procedure

1. Any request for an investigation under Article 5(b) above, shall be addressed to the DPO in writing.
2. The DPO shall send acknowledgment of receipt to the requester within five working days. In the event of manifest abuse of the right to request an investigation, the DPO shall inform the applicant that the request is not being pursued and give account of the reasons.
3. The DPO may investigate the matter on-site and request a written statement from the controller of the data processing the activity in question. The controller shall provide his/her response to the DPO within five working days. The DPO may ask for additional information or assistance from any other EUDA staff member whose activities are related to the processing operation in question. The staff member shall provide requested information or assistance within five working days of the DPO's request.
4. The DPO shall report back to the requester within one calendar month of the receipt of the request.
5. 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.

SECTION 5
FINAL PROVISION

Article 13
Entry into force

This Decision shall enter into force on the date following its adoption by the Management Board of the EUDA. It will be published on the EUDA's Intranet.

Done in Lisbon, on 6 December 2024.

For the Management Board

The Chairperson

Franz Pietsch