

DECISION 01/2020
OF THE DIRECTOR OF
THE EUROPEAN INSTITUTE OF INNOVATION AND TECHNOLOGY (EIT)

ON THE IMPLEMENTING RULES CONCERNING THE DATA PROTECTION OFFICER
OF THE EUROPEAN INSTITUTE OF INNOVATION AND TECHNOLOGY

THE DIRECTOR OF THE EUROPEAN INSTITUTE OF INNOVATION AND TECHNOLOGY,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Article 8 thereof,

Having regard to Regulation (EC) No 294/2008 of the European Parliament and of the Council of 11 March 2008 establishing the European Institute of Innovation and Technology¹, as amended by Regulation (EU) No 1292/2013 of the European Parliament and of the Council of 11 December 2013² (hereinafter "EIT Regulation"), in particular Article 13(5) thereof,

Having regard to Regulation (EC) 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/EC³ (hereinafter "Regulation 2018/1725"), and in particular Article 45(3) thereof;

WHEREAS

- (1) The Treaty on the Functioning of the European Union and the Charter of Fundamental Rights of the European Union provide for the right to the protection of personal data;
- (2) Regulation 2018/1725, in particular Article 43(1) obliges all Union institutions, agencies and bodies to designate a data protection officer (hereinafter "DPO");
- (3) Under Article 45(3) of Regulation 2018/1725 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 DPO.

¹ OJ L97 of 09.04.2008, p. 1.

² OJ L347 of 20.12.2013, p. 174.

³ OJ L295/39, 21.11.2018

HAS DECIDED AS FOLLOWS:

Article 1
Adoption

This decision lays down the implementing rules concerning to the Data Protection Officer of the EIT, as defined in the Annex.

Article 2
Entry into force

This decision shall enter into force on the day of its signature.

Done in Budapest on 13 January 2020

Martin Kern

Director of the EIT

IMPLEMENTING RULES CONCERNING THE DATA PROTECTION OFFICER

Section 1 General provisions

Article 1 Subject matter and scope

For the purposes of these internal rules implementing Regulation (EU) No 2018/1725 (hereinafter “Regulation”), the definitions set out in Article 3 of the aforementioned Regulation shall apply.

Section 2 The Data Protection Officer (DPO)

Article 2 Designation, status and independence of the DPO

1. The Director of EIT (hereinafter referred to as “Director”) shall appoint the DPO from the members of the EIT staff and register him/her with the European Data Protection Supervisor (hereinafter referred to as “EDPS”). The contact details of the DPO shall be published on the EIT website.
2. The DPO shall be designated on the basis of professional qualities, in particular, expert knowledge of data protection law and practices, the EIT administrative rules and procedures, information systems, and the abilities to fulfil the tasks referred to in Article 45 of the Regulation.
3. The term of office of the DPO shall be for a period of three up to five years by decision of the Director. The DPO shall be eligible for reappointment.
4. The DPO may be dismissed by the EIT Director if he/she no longer fulfils the conditions required for the performance of his/her duties and only with the consent of the EDPS. DPO shall be dismissed at the request of himself/herself as well for reasons that do not compromise the exercise of his or her functions.
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 other tasks. The Director 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.
6. The DPO shall be independent in the performance of his/her duties. He/she may not receive any instructions from the Governing Board or the Director of the EIT or from anyone regarding the

exercise of the DPO's tasks. The DPO shall not suffer any prejudice on account of the performance of his/her duties.

Without prejudice to such independence, the DPO shall be subject to the provisions applicable to EIT staff.

In addition, without prejudice to the provisions of the Regulation concerning his or her independence and obligations, the DPO shall report directly to the Director. 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 Director shall ensure an equal and fair treatment.

7. The DPO shall be bound by secrecy or confidentiality concerning the performance of his/her tasks in accordance with Union law.
8. A Deputy DPO may be designated (and dismissed) 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.
9. EIT staff assisting the DPO on data protection matters may be appointed, after consultation with the DPO. While performing their tasks on data protection issues, he/she shall act solely on the DPO's instructions and shall be bound by the same duty of secrecy and confidentiality as the DPO as regards any confidential documents or information obtained in the course of his/her duties.
10. The EIT shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. Under Article 44(2) of the Regulation the EIT shall support the DPO in performing his/her tasks set out in Article 45 of the Regulation and in Articles 3 and 4 of this Decision and provide with the necessary resources.

Article 3 **Tasks and duties**

When carrying out the tasks specified in Article 45 of the Regulation, the DPO shall:

1. Inform and advise the Controller⁴ or the processor⁵ and the EIT responsible staff who carry out processing of their obligations pursuant to the Regulation and to any relevant data protection rules applicable to European Union institutions, agencies and bodies;
2. Ensure that data subjects are informed of their rights and obligations pursuant to the Regulation;
3. Ensure in an independent manner the application of the Regulation within that EIT; to monitor compliance with the Regulation, with the relevant data protection rules and with the policies of the Controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of EIT staff involved in processing operation, and the related audits;

⁴ See Article 3(8) of the Regulation. In case of the EIT, the controller can be the Director of the EIT or the Heads of Unit.

⁵ See Article 3(12) of the Regulation. In case of the EIT, the processor can be an external service provider.

4. Provide advice where requested on the necessity for a notification or a communication of a personal data breach pursuant to the Articles 34 and 35 of the Regulation;
5. Provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 of the Regulation and to consult the EDPS in case of doubt as to the need for a data protection impact assessment (hereinafter “DPIA”);
6. Provide advice where requested as regards the need for prior consultation of the EDPS pursuant to Article 40 of the Regulation, including consultation in case of doubt as to the need for a prior consultation;
7. Respond to requests from the EDPS; within the sphere of his/her competence, to cooperate and consult with the EDPS at the latter’s request or on his/her own initiative;
8. Ensure that the rights and freedoms of data subjects are not adversely affected by processing operations;
9. Keep a centralised and publicly available register of records of processing activities in accordance with the Article 31(5) of the Regulation;
10. Report any breach, including personal data breach, of the provisions of the Regulation to the EIT’s Director. The DPO shall bring to the Director’s attention any serious failure of a staff member to comply with the obligations pursuant to the Regulation and propose an administrative inquiry with a view to a possible disciplinary action as specified in the Staff Regulations;
11. Regularly attend meetings with the EDPS and/or the DPOs of the other Union institutions and bodies with an aim to establish a mutual exchange of information and experience and harmonize the enforcement of the Regulation within the Union institutions and bodies;
12. Act as Controller for processing operations on personal data under his/her responsibility;
13. Shall include a brief summary of the data protection activities of the previous year in the Annual Activity Report of the EIT;
14. In exercising his/her tasks and powers, the DPO shall take into account the Guidelines on the different matters issued by the EDPS.

Article 4 Powers

In carrying out his/her tasks and duties in accordance with the Regulation, the DPO:

1. May request clarifications from EIT staff or EIT bodies on any matter related with the DPO tasks and duties;
2. Shall be able to obtain access to the data forming the subject matter of processing operations on personal data and to all offices, data processing installations and data carriers including those of processors;

3. May make recommendations for the practical improvement of data protection in the EIT and advise the EIT bodies, units and third parties, including Controllers or processors, on matters concerning the application of data protection provisions. The DPO may be consulted directly without going through official channels on any issue concerning the interpretation or application of the Regulation by the EIT bodies, units and third parties, including Controllers or processors, the EIT staff;
4. May issue an opinion on his/her initiative on the lawfulness of actual or proposed data processing operations and on measures required in order to ensure that such operations are lawful, and on the suitability or inadequacy of data protection measures in the EIT;
5. May perform investigations at the request of the Controller or the processor, the Staff Committee or any individual, or upon his/her own initiative into matters and occurrences directly relating to his/her tasks, and report back to the applicant who commissioned the investigation or to the Controller, in accordance with the procedure described in Article 5 hereof. If the applicant is a data subject asking for an investigation on the processing of his/her personal data, or if the applicant acts on behalf of the data subject concerned, the DPO must, to the extent possible, ensure confidentiality on the request, unless the data subject concerned gives his or her unambiguous consent for the request to be handled otherwise.
6. 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 Director before referring the matter to the EDPS;
7. Shall have the support and assistance of the IT services of the EIT, including those provided to the EIT by external organisations, and may request technical opinions from the Local Information Security Officer;
8. May participate in the EIT's IT Steering Committee (ITSC) whenever issues relating to the processing of personal data are in agenda. The DPO may propose relevant points in the agenda of the ITSC.

Article 5

Investigation procedure carried out by the DPO

1. Any request for an investigation under Article 4(5) of this Decision shall be addressed to the DPO in writing.
2. The DPO shall send an acknowledgement of receipt to the requestor within 15 working days and verify whether the request is to be treated as confidential. In case of an obvious misuse 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 shall request a written statement on the matter from the Controller who is responsible for the data processing operation in question. The Controller shall provide a response to the DPO within 15 working days. The DPO may ask for additional information or assistance from any EIT unit or staff member to be provided within 15 working days.

4. The DPO shall report back to the requestor within 3 months following its receipt. This period may be suspended until the DPO obtains any further information that he/she may have requested.
5. In case of a serious case with extreme urgency or in order to protect the rights and freedoms of the data subject, the deadlines indicated above may be shortened by the DPO.
6. No one shall suffer prejudice on account of a matter brought to the attention of the DPO alleging a breach of the provision of the Regulation.

Section 3

Staff responsible for the processing operation, including the controller; processors of personal data

Article 6

Staff responsible for activities processing personal data

1. Staff responsible for the processing operation, including the controller, shall ensure that all the processing operations concerning personal data are performed in accordance with the Regulation.
2. Without prejudice to the provisions of the Regulation concerning his/her obligation, responsible staff shall:
 - a) Notify and involve, as appropriate, the DPO as of planning phase of any activity processing personal data;
 - b) Inform the DPO without undue delay about any data processing operation, and in any case before undertaking it, if possible;
 - c) Establish the record of processing activities in accordance with Article 31(1) of the Regulation and the related privacy statement, and maintain them under his/her responsibility;
 - d) Transmit the record to the EIT's register of processing activities as referred to in Article 31(5) of the Regulation and Article 9 of the present decision;
 - e) 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;
 - f) Implement appropriate technical and organisational measures to ensure and be able to demonstrate that all the processing operations involving personal data performed with his/her area of responsibility comply with the provisions of the Regulation;
 - g) Seek for advice of the DPO on need of a prior consultation of the EDPS according to Article 40(1) of the Regulation;

- h) Inform the DPO without undue delay about the cases of personal data breach;
 - i) Assist the DPO (and the EDPS, if requested) in the performance of their tasks and duties, and particularly provide them with the full information, grant access to the personal data and respond to the questions within 15 working days from the receipt of the request;
 - j) Ensure that any operations delegated to a processor are processed in compliance with the requirements of Articles 29 and 30 of Regulation.
3. In case of personal data breach, the Local Information Security Officer shall inform the responsible staff as well as the DPO without undue delay, including when they have doubts on whether personal data are affected by the security breach. The Local Information Security Officer shall provide the DPO with all the necessary information enabling his/her to ensure that the EIT complies with the Regulation, and more specifically with the obligation on personal data breach notifications and communications of Articles 34 and 35 of the Regulation.

Article 7 Joint controllers

1. Formal arrangements shall be concluded with joint controllers, as referred to in Article 28 of the Regulation, in order to allocate responsibilities for compliance with the Regulation. Responsible staff shall consult the DPO on those draft agreements. The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. Irrespective of the terms of the arrangement, the data subject may exercise his/her rights under the Regulation in respect of and against each of the controllers.

Article 8 Processor

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

Article 9 Register

1. The register mentioned in Article 6(2)(d) of the present decision is a repository of the EIT which contains of all the records of activities processing personal data submitted by the responsible staff.
2. The register shall be accessible in electronic format and on paper in the EIT premises. The electronic format shall also be published on the EIT website.

3. Any individual can request an extract from the register in writing to the DPO, who shall respond to the request within 15 working days.

Section 4 Data subjects' rights

Article 10 Exercise of data subjects' rights

1. When data subjects contact the EIT to exercise their rights pursuant to Article 17-24 of the Regulation:
 - a. The responsible staff shall consult the DPO before acting in reply to the data subject's request;
 - b. The DPO may act as responsible staff for managing data subjects' requests. If this is the case, it may be detailed in Standard Operating Procedure (SOP).

Article 11 Restrictions

1. Data subject rights provided by Articles 14 to 22 of the Regulation as well as by Articles 35 and 36, may be restricted based on EIT internal rules under Article 25(1) of the Regulation. Responsible staff shall seek the advice of the DPO when planning to apply these restrictions.