**DECISION OF THE BOARD OF THE EUROPEAN UNION INSTITUTE FOR SECURITY STUDIES**

**adopting implementing rules concerning the tasks, duties and powers of the Data Protection Officer pursuant to Article 24.8 of Regulation (EC) No 45/2001 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**

**The Board of the European Union Institute for Security Studies**

Having regard to Council Decision 2014/75/CFSP of 10 February 2014 on the European Union Institute for Security Studies and in particular Article 18 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[1], and in particular Article 24(8) and the Annex thereof,

Having regard to the Director's proposal,

Whereas:

Article 16 of the Treaty on the Functioning of the European Union enshrines the right to the protection of personal data.

Regulation (EC) No 45/2001, hereinafter referred to as the 'Regulation', sets out the principles and rules applicable to all European Union institutions and bodies and provides for the appointment by each institution and body of a Data Protection Officer.

Article 24.8 of the Regulation requires that further implementing rules concerning the Data Protection Officer shall be adopted by each European institution or body in accordance with the provisions in the Annex. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer.

**Has decided as follows:**

*Article 1*
*Definitions*

Without prejudice to the definitions provided in Article 2 of the Regulation:

[1] OJ L 8, 12.1.2001, p.1.

‘Data subject’ shall mean the identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

‘Controller’ shall mean the European Union Institute for Security Studies, hereinafter referred to as the ‘EUISS’, which alone or jointly with others determines the purposes and means of the processing of personal data and is legally responsible for such processing operations.

‘Person designated as being in charge of the processing operation’ shall mean the person responsible, in practice, for internally managing the processing operation.

*Article 2*
*Scope*

1. This decision defines the rules and procedures for implementation of the function of Data Protection Officer (hereinafter referred to as the ‘DPO’) within the EUISS pursuant to Article 24.8 of the Regulation. It shall apply to all activities in relation to the processing of personal data by or on behalf of the EUISS.

2. This decision also lays down the general rules pursuant to which a data subject may exercise his or her rights.

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

1. The Director shall appoint the DPO and register him or her with the European Data Protection Supervisor (hereinafter referred to as the ‘EDPS’). An assistant DPO may be appointed in accordance with the same procedure and for the same term, to assist the DPO in all the latter's duties.

2. The term of office of the DPO shall be for a period of three years, renewable up to a maximum total term of nine years.

3. The DPO shall act in an independent manner with regard to the internal application of the provisions of the Regulation and may not receive any instructions. His or her selection shall not be liable to result in a conflict of interest between his or her duty as DPO and any other official duties, in particular in relation to the provisions of the Regulation. To the extent required, the DPO shall be relieved of other activities. In case of an assistant DPO, the same guarantees of independence must be enshrined in the document.

4. The DPO shall be selected on the basis of his or her personal and professional qualities and, in particular, his or her expert knowledge of data protection. Additionally, the DPO should have a sound knowledge of the administrative rules and procedures. The DPO must have the capacity to demonstrate sound judgement

and the ability to maintain an impartial and objective stance in accordance with the Staff Regulations.

5. Without prejudice to the provisions of the Regulation concerning his or her independence and obligations, the DPO shall report directly to the Director.

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

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

*Article 4*
*Tasks and duties of the Data Protection Officer*

1. Without prejudice to the tasks as described in Article 24 of the Regulation and in its Annex, the DPO shall raise awareness on data protection issues and encourage a culture of protection of personal data within the EUISS. The DPO shall ensure that persons designated as being in charge of the processing operations and data subjects are informed of their rights and obligations pursuant to the Regulation.

2. The DPO shall respond to requests from the EDPS and, within the sphere of his or her competence, cooperate with the EDPS at the latter's request or on his or her own initiative.

3. The DPO may maintain an inventory of all processing operations on personal data of the EUISS and may introduce therein, in cooperation with the persons designated as being in charge of the processing operations, all processing operations to be notified.

4. The DPO shall assist the persons designated as being in charge of the processing operations in the preparation of notifications and shall notify the EDPS of the processing operations likely to present specific risks within the meaning of Article 27 of the Regulation. In case of doubt as to the need for prior checking, the DPO shall consult the EDPS as stated in Article 27.3.

5. Pursuant to Article 26 of the Regulation, the DPO shall keep a register of the processing operations carried out by the controller, containing the items of information referred to in Article 25.2.

6. The DPO may keep an anonymous inventory of the written requests from data subjects for the exercise of the rights referred to in Article 13, 14, 15, 16 and 18 of the Regulation.

7. The DPO may be consulted by any person employed by the EUISS, without going through the official channels, on any matter concerning the interpretation or application of the Regulation.

8. The DPO may make recommendations and give advice on matters concerning the application of data protection provisions and may perform investigations on request, or upon his or her own initiative, into matters and occurrences 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 the procedure described in Article 12 hereof. If the applicant is an individual, or if the applicant acts on behalf of an individual, the DPO must, to the extent possible, ensure confidentiality governing the request, unless the data subject concerned gives his or her unambiguous consent for the request to be handled otherwise.

9. Without prejudice to the independence of the DPO, the Director may ask the DPO to represent the EUISS on any data protection issues, including participation in inter-institutional committees and bodies.

10. In addition to his or her tasks within the EUISS, the DPO shall cooperate in carrying out his or her functions with the DPOs of other institutions and bodies, in particular by exchanging experience and best practices. He or she shall participate in the dedicated network(s) of DPOs.

11. For processing operations on personal data under his or her responsibility, the DPO shall act as the person designated as being in charge of these processing operations.

*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 Regulation, the DPO:

   a) May request legal opinions from the EDPS on data protection issues;

   b) May, in the event of disagreement relating to the interpretation or implementation of the Regulation, inform the Director before referring the matter to the EDPS;

   c) May bring to the attention of the Director any failure of a staff member to comply with the obligations under the Regulation. Subsequently, the DPO may suggest that an administrative investigation be launched with a view to possible application of Article 49 of the Regulation;

   d) May investigate matters and occurrences directly relating to the tasks of the DPO, applying the appropriate principles for inquiries and audits in the EUISS and the procedure described in Article 12 thereof.

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 carriers.

3. Every person designated as being in charge of processing operations and employed by the EUISS shall be required to assist the DPO in performing his or her duties and to give information in reply to questions.

*Article 6*
*Resources of the Data Protection Officer*

Resources (both in terms of time availability, HR, IT and finance) shall be provided to the DPO to carry out properly his or her duties. The DPO should benefit from the necessary training and should have the opportunity to update his or her knowledge with regard to the legal and technical aspects of data protection.

*Article 7*
*Information of the Data Protection Officer*

The DPO should be informed whenever the EUISS consults the EDPS under Articles 28.1, 28.2 or 46.d (and more generally be informed of any correspondence with the EDPS). The DPO should be informed of direct interactions between the persons designated as being in charge of processing operations and the EDPS. The DPO should be informed before any opinion, document or internal decision on matters related to data protection provisions is adopted by the EUISS.

The DPO should be informed when the controller receives a request for access, rectification or deletion, as well as any complaint related to data protection matters.

*Article 8*
*Person designated as being in charge of processing operations*

1. Without prejudice to the responsibility of the controller, the person designated as being in charge of processing operations shall ensure that all processing operations involving personal data within his or her area(s) of responsibility comply with the Regulation. For that purpose he or she shall give prior notice to the DPO of any processing operation, in accordance with the provisions described in Article 10 hereof.

2. Without prejudice to the provisions of the Regulation concerning the obligations of the controller, the person designated as being in charge of processing operations shall:

    a) Give prior notice to the DPO of any processing operation;

    b) Notify promptly any change in processing operations implying personal data;

    c) Cooperate with the DPO to establish the inventory of processing operations referred to in Article 4(3) hereof;

d) Where appropriate, consult the DPO on the conformity of processing operations, in particular in the event of doubt as to the conformity;

e) Prepare without delay notifications containing items listed in Article 25.2 to the DPO for all existing processing operations which have not yet been notified.

*Article 9*
*Processors*

Formal contracts shall be concluded with external processors; such contracts shall contain all the specific requirements mentioned in Article 23.2 of the Regulation.

*Article 10*
*Notifications to the Data Protection Officer*

1. Before introducing new processing operations relating to personal data, the relevant person designated as being in charge of these processing operations shall give notice to the DPO. The inventory referred to in Article 4.3. hereof may be used as a guidance instrument for planning the notification exercise.

2. Any processing operations that are likely to present specific risks under Article 27 of the Regulation shall be notified by the DPO sufficiently well in advance to allow for prior checking by the EDPS. The operation cannot be implemented before the prior checking of the EDPS has taken place.

3. The notification shall include all information required in Article 25.2 of the Regulation.

4. For the submission of their notifications to the DPO, the persons designated as being in charge of processing operations shall use the notification forms.

*Article 11*
*Register*

1. The register mentioned in Article 4.5. hereof is the database of the EUISS which contains all the processing operations submitted by the persons designated as being in charge of these operations to the DPO pursuant to Article 25 of the Regulation.

2. The register shall be accessible in electronic and paper format. The electronic format may be published on the EUISS website as well.

3. Extracts of the register can be requested by any person in writing to the DPO, who shall reply within 15 working days.

*Article 12*
*Investigation procedure*

1. The requests for an investigation mentioned in Article 4.8. hereof shall be addressed to the DPO in writing. Within 15 days of receipt, the DPO shall send an acknowledgment of receipt to the person who commissioned the investigation, and verify whether the request is to be treated as confidential. In the event of manifest abuse of the right to request an investigation, for example where it is repetitive, abusive and/or pointless, the DPO may inform the applicant that the request will not be pursued.

2. The DPO shall request a written statement on the matter from the person designated as being in charge of the processing operation in question. The person designated as being in charge of the processing operation shall provide a response to the DPO within 15 working days. The DPO may request complementary information from the person designated as being in charge of the processing operation and/or from other parties within 15 working days. The DPO shall be provided with the opinion within 20 working days.

3. The DPO shall report back to the person who requested the investigation no later than three months following its receipt. This period may be extended until the DPO has obtained any further information that may have been requested.

4. 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 13*
*General rules governing the exercise of rights by data subjects*

1. Further to their right to be appropriately informed according to Articles 11 and 12 of the Regulation, data subjects may approach the relevant person designated as being in charge of the processing operation to exercise their rights pursuant to Articles 13 to 19 of the Regulation, as specified below:

    a) 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.

    b) Requests to exercise these rights shall be addressed in writing to the relevant person designated as being in charge of the processing operation. The person shall only grant the request if the applicant's identity and, if relevant, his or her entitlement to represent the data subject have been appropriately verified. The person designated as being in charge of the processing operation 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 person designated as being in charge of the processing operation shall include the grounds for the rejection.

c) The person designated as being in charge of the processing operation shall as soon as possible, but at the latest within three calendar months of receipt of the request, grant access pursuant to Article 13 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.

d) Data subjects may contact the DPO in the event that the person designated as being in charge of the processing operation does not respect either of the time limits in paragraphs (b) or (c). In the event of manifest abuse by a data subject in exercising his or her rights, the person designated as being in charge of the processing operation may refer the data subject to the DPO. If the case is referred to the DPO, the DPO shall decide on the merits of the request and the appropriate follow-up. In the event of disagreement between the data subject and the person designated as being in charge of the processing operation, both parties shall have the right to consult the DPO.

2. Any person employed by the EUISS may firstly lodge a complaint at local level with the DPO before eventually referring to the EDPS pursuant to Article 33 of the Regulation.

*Article 14*
*Entry into force*

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

Done in Brussels, on 28/07/2014.