Brussels, 12 October 2010

DECISION OF THE EUROPEAN DATA PROTECTION SUPERVISOR

adopting implementing rules concerning the Data Protection Officer pursuant to Article 24(8) of Regulation (EC) N° 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 EUROPEAN DATA PROTECTION SUPERVISOR

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,

Whereas:

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

(2) 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.

(3) Article 24(8) of the Regulation requires that further implementing rules concerning the Data Protection Officer shall be adopted by each European Union 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:

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

Article 1
Definitions

For the purpose of this Decision, and without prejudice to the definitions provided for by the Regulation, “institution" shall mean the institution of the European Data Protection Supervisor (hereinafter referred to as the “EDPS”).

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 institution 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 institution.

2. The 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

1. The DPO shall be appointed by and registered with 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].

2. The term of office of the DPO shall be for a period of two up to five years, renewable up to a maximum total term of ten 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 with respect to the performance of his or her duties. The selection of the DPO shall not result in a conflict of interests between his or her duty as DPO and any other official duties, in particular in relation to the application of the provisions of this Regulation.

4. The DPO shall be selected from the staff of the institution. The DPO should have a sound knowledge of data protection and of the institution's 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. 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 his or her specific DPO duties), for which the Director shall ensure equal and fair treatment.

[2] Where an Assistant DPO is appointed pursuant to this procedure the expression "DPO" shall be understood in this Decision to mean both the DPO and the Assistant DPO

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

7. In accordance with the Regulation, the DPO may be dismissed from the post of DPO, but only with the consent of both the European Data Protection Supervisor and the Assistant Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.

Article 4
Tasks and Duties

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, particularly within the services involved in the processing of personal data.

2. The DPO shall maintain an inventory of all processing operations on personal data of the institution and shall introduce therein, in cooperation with the controllers, all processing operations to be notified. The DPO shall help the controllers to assess the risk of the processing operations under their responsibility. The DPO shall monitor implementation of the Regulation in the institution in particular through a yearly Data Protection Status Report.

3. The DPO shall assist the controller in the preparation of notifications, and where required shall submit to the EDPS the prior checking notifications submitted pursuant to Article 27 of the Regulation.

4. The DPO shall keep the register of processing operations, provided for in Article 26 of the Regulation, available at the institution in electronic and paper format.

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

6. The DPO may make recommendations and give advice to controllers on matters concerning the application of the 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 other tasks, and report back to the person who commissioned the investigation, 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.

7. Processing of personal data by the Staff Committee shall fall within the remit of the DPO.

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

9. In addition to his or her tasks within the institution, 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.

10. The DPO is responsible for responding to requests from the EDPS and, within his or her sphere of competence, for cooperating with the EDPS at the latter's request or on his or her own initiative.

11. For processing operations on personal data under his or her responsibility the DPO shall act as controller.

Article 5
Powers

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 relevant Head of Sector of the EDPS;

   (b) May, in the event of disagreement relating to interpretation or implementation of the Regulation, inform the competent Head of Sector and the Director before referring the matter to the European Data Protection Supervisor and the Assistant Supervisor;

   (c) May bring to the attention of the Director any failure of a staff member to comply with the obligations under the Regulation and with the institution's Internal Control Standards more specifically related to 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 institution and the procedure described in Article 12 hereof;

   (e) 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;

   (f) The DPO shall have the support and assistance of the IT services of the EDPS, including those provided to the institution, and may request technical opinions from the Local Information Security Officer.

2. Every controller and member of the institution's staff concerned shall be required to assist the DPO in performing his or her duties and to give information in reply to questions.

Article 6
Resources

The institution shall provide the DPO with the necessary resources to carry out his or her tasks and duties. The DPO should have access to 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

1. The DPO shall be informed on direct interactions between the controllers of the institution and the EDPS pursuant to the relevant Articles of the Regulation.

2. 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 personal data and the processing thereof, and related to access to information.

3. The DPO shall submit an annual report on his or her activities and on the state of play as regards the data protection activities and compliance of the institution. The DPO shall produce a summary of this report to contribute to the Annual Activity Report of the EDPS.

4. The DPO shall inform the Director by means of a periodical report and dedicated meetings.

Article 8
Controllers

1. Controllers shall ensure that all processing operations involving personal data within their area(s) of responsibility comply with the Regulation. For that purpose they shall give prior notice to the DPO of any processing operation, in accordance with the provision described in Article 10 hereof.

2. Without prejudice to the provisions of the Regulation concerning their obligations, controllers shall:

   (a) Cooperate with the DPO to establish the inventory of processing operations referred to in Article 4(2) hereof;

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

(c) Prepare without delay notifications to the DPO for all existing processing operations which have not yet been notified;

(d) Maintain anonymous lists of written requests from data subjects for the exercise of the rights referred to in Articles 13, 14, 15, 16 and 18 of the Regulation. These lists shall be transmitted to the DPO to feed in the inventory described in Article 4(5) hereof.

Article 9
Processors

Formal contracts shall be concluded with external processors; such contracts shall contain the specific requirements mentioned in Article 23(2) of the Regulation.

Article 10
Notifications

1. Before introducing new processing operations relating to personal data, the relevant controller shall give notice to the DPO. The inventory referred to in Article 4(2) hereof may be used as 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 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 notifications shall include all information required in Article 25(2) of the Regulation.

4. For the submission of their notifications to the DPO, controllers shall use the notification forms. The original signed paper notifications shall reach the DPO's office premises.

5. Controllers shall immediately inform the DPO of any change affecting the information contained in a notification already submitted.

6. The DPO shall provide practical guidance and assistance to controllers.

Article 11
Register

1. The register mentioned in Article 4(4) hereof is the database of the institution which contains all the final notifications submitted by controllers to the DPO pursuant Article 25 of the Regulation.

2. The register shall be accessible through the institution's website, and on paper format in the DPO's office premises. An index of the content of the register will be published on the institution's website.

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(6) hereof shall be addressed to the DPO in writing. Within 15 days upon 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 controller responsible for the data-processing operation in question. The controller shall provide a response to the DPO within 15 working days. The DPO may request complementary information from the controller and/or from other parties within 15 working days. If appropriate the DPO may request an opinion on the issue from the relevant Head of Sector of the EDPS. 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 suspended 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 about any processing of their personal data, data subjects may approach the relevant controller to exercise their rights pursuant to Articles 13 to 19 of 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 controller. The controller 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

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.

(c) The controller 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 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 controller 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 controller 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 controller, both parties shall have the right to consult the DPO.

2. The members of the institution's staff may consult the DPO before lodging a complaint with the EDPS pursuant to Article 33 of the Regulation.

Article 14
Entry into Force

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

2. After entry into force, this Decision will be published on the EDPS website.

Done in Brussels on 12 October 2010

The European Data Protection Supervisor

Peter HUSTINX