

II

(Acts adopted under the EC Treaty/Euratom Treaty whose publication is not obligatory)

DECISIONS

COMMISSION

COMMISSION DECISION

of 3 June 2008

adopting implementing rules concerning 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

(2008/597/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

HAS DECIDED AS FOLLOWS:

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) Regulation (EC) No 45/2001, hereinafter referred to as the 'Regulation', sets out the principles and rules applicable to all Community institutions and bodies and provides for the appointment by each Community institution and Community body of a Data Protection Officer.
- (2) Article 24(8) of the Regulation requires that further implementing rules concerning the Data Protection Officer shall be adopted by each Community 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.
- (3) Commission Decision C(2002) 510 ⁽²⁾ of 18 February 2002 creates the post of Data Protection Officer (DPO) for the Commission and charges the DPO with proposing further implementing rules following consultation with the Directorates-General according to their needs and experiences,

SECTION 1

GENERAL PROVISIONS

Article 1

Definitions

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

- 'Data Protection Coordinator' (hereinafter referred to as the 'DPC') shall mean the staff member within a Directorate-General or Service who has been appointed by the Director-General to coordinate all aspects of the protection of personal data in the Directorate-General,
- 'Controller', as defined in Article 2(d) and referred to in Article 25(2)(a), shall mean the official responsible for the organisational unit that has determined the purposes and the means of the processing of personal data.

Article 2

Scope

This Decision defines the rules and procedures for implementation of the function of Data Protection Officer (hereinafter referred to as the 'DPO') within the Commission pursuant to Article 24(8) of the Regulation. It shall not apply to the activities of the Commission when defining policies relating to the protection of individuals with regard to the processing of personal data.

⁽¹⁾ OJ L 8, 12.1.2001, p. 1.

⁽²⁾ Not yet published in the Official Journal.

SECTION 2

THE DATA PROTECTION OFFICER

Article 3

Appointment and status

1. The Commission shall appoint the DPO ⁽¹⁾ and register him with the European Data Protection Supervisor (hereinafter referred to as the 'EDPS').

2. The term of office of the DPO shall be five years, renewable once.

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 duties.

4. The DPO shall be selected from the staff of the Commission following the relevant procedures. In addition to the requirements of Article 24(2) of the Regulation, the DPO should have a sound knowledge of the Commission services and their structure and administrative rules and procedures. He should have a good knowledge of data protection and information systems, principles and methodologies. He 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. In accordance with the Regulation, the DPO may be dismissed from his post by the Commission, but only with the consent of the EDPS, if he no longer fulfils the conditions required for the performance of his duties. The Commission, upon a proposal from the Secretary-General in agreement with the Director-General for Personnel and Administration, shall establish that the DPO no longer fulfils the conditions required for the performance of his tasks.

6. Without prejudice to the relevant provisions of the Regulation, the DPO and his/her staff shall be subject to the rules and regulations applicable to officials of the European Communities.

Article 4

Tasks

1. Without prejudice to the tasks as described in Article 24 of the Regulation and in its Annex, the DPO shall contribute to creating a culture of protection of personal data within the Commission by raising general awareness of data protection issues while maintaining a just balance between the principles of protection of personal data and transparency.

2. The DPO shall maintain an inventory of all processing operations on personal data of the Commission into which the DPCs introduce, for their respective DG, all processing

operations to be notified. The DPCs shall also identify the Controller responsible of such processing operations. The DPO shall help the Controller to assess the risk of the processing operations under his responsibility and monitor implementation of the Regulation in the Commission, in particular through a yearly Data Protection Status Report.

3. The DPO shall organise and chair the regular meetings of the network of DPCs.

4. The DPO shall make the register of processing operations, provided for in Article 26 of the Regulation, available on the internal and external websites of the Commission.

5. The DPO may make recommendations and give advice to the Commission and the Controllers on matters concerning the application of data protection provisions and may perform investigations on request, or upon his own initiative, into matters and occurrences directly relating to his tasks, and report back to the person who commissioned the investigation, in accordance with the procedure described in Article 13 hereof. If the requester is an individual, or if the requester 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/her unambiguous consent for the request to be handled otherwise.

6. Processing of personal data by Staff Committees shall fall within the remit of the DPO of the Commission. For the purposes of Article 6 below, the DPO shall provide any information to the President of the Staff Committee concerned instead of the Secretary-General, where any question relating to processing operations by the Staff Committee concerned arises.

7. Without prejudice to the independence of the DPO, the Secretary-General, on behalf of the Commission, can ask him to represent the institution in all data protection issues; this may include the DPO's participation in relevant committees and bodies at international level.

Article 5

Duties

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

(a) submit each year a Data Protection Status Report for the Commission to the Secretary-General and the Director-General for Personnel and Administration for discussion at the appropriate level, such as at the regular meeting of Directors-General; the report shall be made available to the Commission's staff;

⁽¹⁾ Each reference to the Data Protection Officer in the following text shall mean he or she and his or her.

(b) cooperate in the discharge of his functions with the DPOs of the other institutions and bodies, in particular by exchanging experience and best practices.

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

Article 6

Powers

In performing his tasks and duties and without prejudice to the powers conferred by the Regulation, the DPO:

(a) may request legal opinions from the Legal Service of the Commission;

(b) may, in the event of conflict relating to interpretation or implementation of the Regulation, inform the competent management level and the Secretary-General before referring the matter to the EDPS;

(c) may bring to the attention of the Secretary-General any failure of:

— a staff member to comply with the obligations under the Regulation,

— controllers to comply with those Commission Internal Control Standards more specifically related to the obligations under the Regulation,

and 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 his tasks, applying the appropriate principles for inquiries and audits in the Commission and the procedure described in Article 13 of this Decision;

(e) 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.

Article 7

Resources

The Commission shall provide the DPO with the necessary resources to carry out his duties.

SECTION 3

RULES AND PROCEDURES

Article 8

Information

1. The DPO shall be informed immediately by the lead service whenever an issue, which has data-protection impli-

cations, is under consideration in the Commission's services, and at the latest prior to taking any decision.

2. When the Commission consults and informs the EDPS under the relevant Articles of the Regulation, and in particular pursuant to Article 28(1) and 28(2), the DPO shall be informed. He shall also be informed on direct interactions between the Controllers of the Commission and the EDPS pursuant to the relevant Articles of the Regulation.

3. The DPO shall be informed by the lead service or by the Legal Service, as appropriate, about opinions and position papers of the Legal Service directly relating to 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 more particularly related to Inter-Service Consultation, and related to access to information.

Article 9

Controllers

1. Without prejudice to the provisions of the Regulation concerning their obligations, Controllers shall:

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

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

(c) cooperate with the DPC to establish the inventory of existing processing operations on personal data of the Directorate-General.

2. The Controller may delegate certain parts of his tasks to other persons acting as a Delegated Controller under his authority and responsibility.

Article 10

Processors

Processors within the Commission, required to process personal data on behalf of Controllers, shall act only on the Controllers' instructions documented in a written agreement and process such personal data in strict compliance with the Regulation, and any other applicable legislation on data protection. A written agreement between organisational units of the Commission shall be considered equivalent to a legally binding act within the meaning of Article 23(2) of the Regulation.

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

Article 11

Notifications

Controllers shall use the online notification system of the Commission, accessible through the website of the DPO on the Commission's Intranet, to submit their notifications to the DPO.

For simple processing operations on non-sensitive personal data, the system shall offer a simplified notification.

Article 12

Register

The electronic register of processing operations of the Commission mentioned in Article 4(4) hereof shall be accessible through the website of the DPO on the Intranet of the Commission for all staff of Community institutions and bodies and on the Europa website for any person having access to the Internet. Extracts of the register can be requested by any person not having access to the Internet in writing to the DPO, who shall reply within 10 working days.

Article 13

Investigation procedure

1. The requests for an investigation mentioned in Article 4(5) hereof shall be addressed to the DPO in writing. Within 15 days upon receipt, the DPO shall send an acknowledgement of receipt to the person who commissioned the investigation, and verify whether the request is to be treated as confidential. In the event of obvious misuse of the right to request an investigation, the DPO shall not be obliged to report back to the requester.

2. 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 his/her response to the DPO within 15 working days. The DPO may wish to receive complementary information from him and/or other parties within 15 days. If appropriate he/she may request an opinion on the issue from the Legal Service. The DPO shall be provided with the opinion within 30 working days.

3. The DPO shall report back to the person who commissioned the investigation no later than three months following its receipt. This period may be suspended until the DPO has obtained any further information that he or she may have 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 14

Data Protection Coordinators

1. A DPC shall be appointed in each Directorate-General or Service by the Director-General or the Head of Service. Based on a written agreement, several Directorates-General, Services or Offices may, for reasons of coherence or efficiency, decide to appoint a common DPC or share the services of an already appointed DPC.

2. The function of DPC can be combined with other functions as appropriate. To acquire the necessary competences for the functions, he must undergo the compulsory training for DPCs within six months of his appointment.

3. The term of office of the DPC shall not be limited. He should be chosen, at the appropriate hierarchical level, on the basis of his high professional ethics, his knowledge and experience of the functioning of his Directorate-General and his motivation for the function. He should have an understanding of information systems principles.

4. Without prejudice to the responsibilities of the DPO, the DPC shall:

(a) establish an inventory of processing operations in the Directorate-General, keep it up to date, and help to define an appropriate risk level for each of the processing operations; he shall use the online Inventory Management System for DPCs put in place for those purposes by the DPO on his website on the Commission's Intranet;

(b) assist the Director-General or Head of Service to identify the respective Controllers;

(c) have the right to obtain from the Controllers necessary and adequate information. This shall not include the right to access personal data processed under the responsibility of the Controller.

5. Without prejudice to the responsibilities of the Controller, the DPC shall:

(a) assist the Controllers in complying with their legal obligations;

(b) help the Controllers to establish notifications;

(c) input the simplified notifications into the online notification system of the DPO.

6. The DPC shall participate in the regular meetings of the DPCs' network, chaired by the DPO, to ensure coherent implementation and interpretation of the Regulation in the Commission and to discuss subjects of common interest.

7. In the execution of his tasks the DPC can ask the DPO for a recommendation, advice or an opinion.

Article 15

Administration and management

1. The DPO shall be administratively attached to the Secretariat-General and his activities shall be integrated into the activity-based budgeting and management process under Activity 7 of the Secretariat-General: Relations with Civil Society, Openness and Information. In this context the DPO shall participate in preparing the Annual Management Plan and the Draft Preliminary Budget of the Secretariat-General.

2. The DPO shall be the reporting officer for the staff of his Secretariat and the Assistant Data Protection Officer. The Deputy Secretary-General shall be the countersigning officer.

3. The DPO shall participate in the management coordination of the Secretariat-General as appropriate.

SECTION 4

FINAL PROVISIONS

Article 16

Entry into force

This Decision enters into force on 3 June 2008.

Done at Brussels, 3 June 2008.

For the Commission

The President

José Manuel BARROSO