European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

2013-093

From: Chair

To: Management Board

Prev. Doc: 2013-085

Subject: **Decision of the Management Board on implementing rules relating to Regulation (EC) No 45/2001 of the European Parliament and of the Council 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**

European Agency for the operational management
of large-scale IT systems in the area of freedom, security and justice

Decision of the Management Board on implementing rules relating to Regulation (EC) No 45/2001 of the European Parliament and of the Council 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

Decision of the Management Board on implementing rules relating to Regulation (EC) No 45/2001 of the

European Parliament and of the Council 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 Management Board,

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 and(referred to hereinafter as "*the Regulation*"), in particular, Article 24(8) thereof,

Having regard to the Regulation No 1077/2011 of the European Parliament and the Council of 25 October 2011 (referred to hereinafter as "*eu-LISA Regulation*") establishing a European Agency for the operational management of large scale IT systems in the area of freedom, security and justice,

Whereas:

(1) The Treaty on the Functioning of the European Union and, in particular, Article 16 states that everyone has the right to the protection of personal data concerning them.

(2) The Regulation lays down the principles and the rules applicable to all the Union institutions and bodies and provides for a Data Protection Officer ("*DPO*") to be appointed by each Union institution and body.

(3) Pursuant to Article 24(8) of the Regulation and its Annex, further implementing rules shall be adopted by each Union institution or body in accordance with the provisions set out in the Annex to the Regulation. The implementing rules shall concern in particular the Data Protection Officer's tasks, duties and powers.

(4) The purpose of the Implementing Rules is to lay down procedures which will enable data subjects to exercise their rights and all persons within the Union institutions or bodies who are involved in the processing of personal data to fulfil their obligations.

(5) Pursuant to Article 28 of the eu-LISA Regulation, the Management Board shall establish measures for the application of the Regulation by the Agency.

(6) The European Data Protection Supervisor has issued guidelines on implementing rules concerning the tasks, duties and powers of the Data Protection Officer, and the network of Data Protection Officers has issued professional standards for Data Protection Officers.

(7) The European Data Protection Supervisor has been consulted and provided advice on the drawing up of these internal implementing rules according to Article 46(d) of the Regulation

Has adopted the following Decision:

Article 1
Purpose and definitions

1. This Decision lays down the general rules governing the implementation of the Regulation to cover all processing of personal data by eu-LISA, without prejudice to the provisions on data protection laid down in the legislative instruments governing the development, establishment, operation and use of large-scale IT systems whose operational management has been entrusted to eu-LISA by the eu-LISA Regulation. In particular, it supplements the provisions set out in the Regulation which relate to the tasks, duties and powers of eu-LISA's Data Protection Officer.

2. Furthermore, the Decision lays down the detailed rules pursuant to which a data subject may exercise his or her rights, the procedure for notifying a processing operation and the procedure for obtaining access to the register of processing operations kept by the Data Protection Officer.

3. Without prejudice to Article 19(1) eu-LISA's Data Controller is the Agency itself.

Article 2
Appointment, statute and independence

1. As laid down in Article 12(1)(r) of the eu-LISA Regulation, the Management Board shall appoint the Data Protection Officer. The appointment is done on the basis of his or her personal and professional qualities and, in particular, his or her expert knowledge of data protection. The Data Protection Officer shall report to the Management Board in the performance of his or her duties as Data Protection Officer.

2. The Executive Director shall register the Data Protection Officer with the European Data Protection Supervisor.

3. The Data Protection Officer may perform other duties, provided that they do not result in a conflict of interests with the role of Data Protection Officer, particularly in relation to the application of the provisions laid down in the Regulation. To the extent required, the Data Protection Officer shall be relieved of other activities.

4. The Data Protection Officer shall be appointed for a period of between two and five years (the length of term being determined primarily by the term of the contract of employment) which is renewable subject to a maximum term of ten years.

5. The Data Protection Officer may be dismissed from his or her post only with the consent of the European Data Protection Supervisor and only if he or she no longer fulfils the conditions required for the performance of his / her duties. The European Data Protection Supervisor shall be consulted in writing and a copy sent to the Data Protection Officer.

6. The Data Protection Officer shall be independent in the performance of his or her duties. In that regard, he or she may not receive any instructions, in particular from the Executive Director, the Head of Administration Unit or any other source as regards the internal application of the provisions laid down in the Regulation or his / her cooperation with the European Data Protection Supervisor. The Data Protection Officer shall refrain from any act which is incompatible with the nature of his or her duties.

7. The Data Protection Officer shall not suffer any prejudice on account of the performance of his or her duties.

8. The Data Protection Officer shall maintain, including once he or she has ceased his or her duties, professional secrecy as regards any confidential documents or information which he or she obtains in the course of his or her duties.

9. In case of appointment of a Deputy DPO, the rules for the DPO shall apply mutatis mutandis to the Deputy DPO.

Article 3
Resources

1. The Executive Director shall ensure that the Data Protection Officer has adequate time and resources, including training, to carry out his or her duties.

2. In accordance with Article 24(6) of the Regulation, the Data Protection Officer shall be provided the staff necessary to carry out his/her duties. The provisions on independence in Article 2 (6) of this Decision apply to staff provided in support to the Data Protection Officers tasks and duties.

Article 4
Duties

1. The Data Protection Officer shall ensure that the provisions laid down in the Regulation are applied within eu-LISA. He or she shall carry out his or her tasks in cooperation with the European Data Protection Supervisor.

2. The Data Protection Officer may be consulted at any time by any person and in particular by data subjects in respect of any matter relating to the application of the Regulation within eu-LISA.

3. The Data Protection Officer shall represent eu-LISA in respect of any matter relating to data protection. He or she may in particular attend meetings of committees or relevant bodies at international level.

Article 5
Tasks

Without prejudice to Article 24 of the Regulation, the Data Protection Officer's tasks shall be as follows:

a) *Provision of information*: the DPO shall inform eu-LISA's Data Controller, staff members responsible for the processing operations and data subjects of their rights and obligations under the Regulation, for which purpose he or she shall provide the necessary information concerning the legislation in force, current procedures and existing notified files, and he or she shall facilitate the exercise of those rights and the fulfilment of those obligations. The DPO will contribute to the Agency's annual activity reports to raise awareness on data protection issues internally and externally and he/she will provide training on data protection matters to staff.

b) *Requests from the European Data Protection Supervisor*: the DPO shall play a role in prior-checking procedures and shall respond to requests from the European Data Protection Supervisor.

c) *Cooperation with the European Data Protection Supervisor*: within his or her area of responsibility, the DPO shall play a role in prior-checking procedures and shall cooperate with the European Data Protection Supervisor at the latter's request or on his or her own initiative, particularly as regards dealing with complaints and carrying out inspections.

d) *Provision of information to the European Data Protection Supervisor*: the DPO shall inform the European Data Protection Supervisor regarding any new development at eu-LISA which has a bearing on the protection of personal data.

e) *Inventory of processing operations and Register of processing operations*: the DPO shall, pursuant to Article 26 of the Regulation, keep an inventory and a register of the processing operations carried out by the Data Controller and staff members responsible for the processing operations and shall ensure that that register may be inspected by any individual.

f) *Notification of processing operations which are likely to present specific risks*: the DPO shall notify the European Data Protection Supervisor of any processing operation which is likely to present specific risks within the meaning of Article 27 of the Regulation. Should there be any doubt regarding the need for a prior check, the Data Protection Officer shall consult the European Data Protection Supervisor.

g) *Upholding data subjects' rights and freedoms*: the DPO shall ensure that processing operations do not undermine the rights and freedoms of data subjects and that no person suffers loss or damage for having brought to the Data Protection Officer's attention a matter which in the view of that person constitutes an infringement of the Regulation.

h) The DPO may be consulted by the Agency, by the controller concerned, by the Staff Committee and by any individual, without going through the official channels, on any matter concerning the interpretation or application of the Regulation.

Article 6
Powers

1. In order to perform his or her tasks and in accordance with the conditions laid down in the Regulation, the Data Protection Officer may:

a) On his or her own initiative, make recommendations to the Data Controller or to staff members responsible for the processing operations on issues concerning the application of the provisions relating to data protection or included in these implementing rules;

b) Investigate issues and facts (on his or her own initiative or at the request of the Data Controller, staff members responsible for the processing operations, eu-LISA's Staff Committee or any individual) which relate directly to his or her powers and responsibilities and which have been brought to his or her knowledge. He or she shall consider them in accordance with the principle of impartiality and with due regard to the rights of the data subjects. The Data Protection Officer shall forward his or her findings to the person who submitted the request and to the Data Controller;

c) Report any breach of the provisions laid down in the Regulation to the Executive Director;

d) Regularly attend meetings with the European Data Protection Supervisor and/or the Data Protection Officers of the other institutions and bodies with a view to establishing a mutual exchange of information, engaging in inter-institutional cooperation and harmonising the application of the procedures in force;

e) Draw up regularly an activity report for the Executive Director, the Management Board and the European Data Protection Supervisor concerning activities relating to the protection of data within eu-LISA. He or she shall make the report accessible to eu-LISA's staff;

f) Issue an opinion on the lawfulness of actual or proposed processing operations, on the measures required in order to ensure that such operations are lawful and on the suitability or inadequacy of data protection or of security measures. The opinion may in particular relate to any issue concerning the notification of data processing operations;

g) keep an anonymous register of requests for the exercise of data subject rights (access, rectifications, etc.) Such a register would allow the DPO to more easily identify processing operations that cause compliance issues.

2. In performing his or her duties, the Data Protection Officer:

a) Shall have access at any time to data being processed, to all premises, all data processing installations and all information media and shall have the power to investigate breaches of data protection;

b) May, without prejudice to the duties and powers of the European Data Protection Supervisor, propose administrative measures to the Executive Director and make general recommendations on the appropriate application of the Regulation;

c) May establish an annual work programme for purposes of planning. For publicity, both this document and the DPO's annual report could be published;

d) May, in particular circumstances, make any other recommendation to the Executive Director, the Management Board and/or all the other parties concerned for the concrete improvement of data protection;

e) May bring to the attention of the Executive Director and the Human Resources and Training Unit any failure by a staff member to comply with the obligations pursuant to the Regulation and propose an administrative inquiry with a view to possible disciplinary action as specified in Article 49 of the Regulation; and

f) May request expert opinions, in particular legal and technical, from relevant areas of eu-LISA on any issue related to his or her tasks and duties.

3. No one shall suffer prejudice on account of bringing a matter to the Data Protection Officer’s attention alleging a breach of the provisions of the Regulation.

4. eu-LISA staff shall cooperate with the Data Protection Officer in the performance of his or her duties without requiring further authorisation.

5. The DPO should be consulted before the adoption of any document related to data protection and he/she should be informed of requests to exercise data subject rights.

Article 7
Procedure for notifying processing operations

1. Before processing any personal data (and in sufficiently good time to enable any prior check within the meaning of Article 27(3) of the Regulation to be carried out), staff members responsible for the processing operations, on behalf of the Data Controller, shall notify the Data Protection Officer thereof, for which purpose he or she should use the notification form available to eu-LISA staff. In any event, the notification shall comply with the provisions laid down in Article 25 of the Regulation. The notification shall be signed by the Data Controller and provided to the Data Protection Officer.

2. The Data Controller and staff members responsible for the processing operations shall, in accordance with the notification procedure laid down in Article 25 of the Regulation, immediately notify processing operations which are already under way on the date of entry into force of this Decision.

3. The information to be provided shall include at least the following:

a) The name and address of the Data Controller, and staff members responsible for the processing operations and an indication of the eu-LISA units which are entrusted with the processing of personal data for a particular purpose;

b) The purpose or purposes of the processing;

c) A description of the category or categories of data subjects and of the data or categories of data relating to them;

d) The legal basis of the processing operation for which the data are intended;

e) The recipients or categories of recipient to whom the data might be disclosed;

f) A general indication of the time limits for blocking and erasure of the various categories of data;

g) The proposed transfers of data to third countries or international organisations and recipients who are subject to the law of a Member State;

h) A general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 of the Regulation in order to ensure that processing is secure; and

i) Information allowing a preliminary assessment to be made of whether a processing operation is subject to prior checking pursuant to Article 27 of the Regulation.

4. The Data Controller and staff members responsible for the processing operations shall immediately inform the Data Protection Officer of any change affecting the information referred to in Article 25 of the Regulation.

Article 8
Register of processing operations

1. The Data Protection Officer shall keep a register of the processing operations notified pursuant to Article 7. The register shall detail all the notified processing operations which have been carried out at eu-LISA. The register may be inspected by any person and shall also facilitate the exercise of the recognised rights of the data subject which are laid down in Articles 13 to 19 of the Regulation.

2. The register shall contain the information referred to in Article 7 (3) (a) to (g) of this Decision.

3. If the Data Protection Officer deems it necessary, he or she may take action to rectify the data contained in the register with a view to ensuring that they are accurate.

Article 9
General rules governing the exercise of rights by data subjects

1. The rights of access, rectification, blocking, erasure and objection may be exercised by the data subject or his or her duly authorised representative only. An electronic form may be made available to eu-LISA staff for this purpose.

2. Requests to exercise the rights under paragraph 1 shall be addressed to the Data Controller. The request shall contain:

a) The name, first name and contact details of the data subject;

b) An indication of the right to be exercised;

c) Where appropriate, supporting documents relating to the request;

d) The category or categories of the data concerned; and

e) The applicant's signature and the date of the request.

3. The request may be submitted in particular by internal or external post, email or fax in such a way that the submission and receipt of the request may be certified. Should the request contain any errors or omissions, the Data Controller may ask for additional information. The Data Controller shall verify the applicant's credentials.

4. The Data Controller shall respond to any request to exercise the rights, even in the absence of the personal data processed in the file. An acknowledgement of receipt shall be sent to the applicant within five working days of the receipt of the request. However, the Data Controller shall not be required to send an acknowledgement of receipt if a substantial reply to the request is provided within the same time limit of five working days. The reply shall be sent by the same means of communication as was used by the data subject unless otherwise indicated in the request.

5. The Data Controller shall notify the data subject of his or her right to lodge a complaint with the European Data Protection Supervisor if that person considers that the rights granted to him or her under the Regulation were infringed when the personal data relating to him or her were processed.

6. The data subjects can address the DPO in case Data Controller does not reply within the set deadlines.

7. The data subject may exercise the rights under paragraph 1 free of charge.

8. Requests to exercise the rights under paragraph 1 may be rejected in the cases referred to in Article 20 of the Regulation, subject to application of Article 17 of this Decision.

Article 10
Right of access

1. The data subject shall have the right to obtain, without constraint, as soon as possible, but no later than three months from the receipt of the request and free of charge from the Data Controller:

a) Confirmation as to whether or not data related to him or her are being processed;

b) Information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;

c) Communication in an intelligible form of the data undergoing processing and of any available information as to their source; and

d) Knowledge of the logic involved in any automated decision process concerning him or her.

2. The data subject may access his or her personal data by any of the following means:

a) On site consultation;

b) Issue of a certified copy drawn up by the data controller;

c) Issue of an electronic copy; and

d) Other means available to the Data Controller and suited to the configuration of the file.

Article 11
Right of rectification

1. The data subject shall have the right to obtain from the Data Controller the rectification without delay of inaccurate or incomplete personal data.

2. Requests for rectification shall specify the data to be rectified and the correction to be made. Where appropriate, a request may be accompanied by supporting documents.

3. If a request for rectification is accepted, it shall be acted upon immediately and the data subject notified thereof. Should a request for rectification be rejected, the Data Controller shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the rejection.

Article 12
Right to have data blocked

1. The data subject shall have the right to obtain from the Data Controller the blocking of data where:

a) Their accuracy is contested by the data subject, for a period enabling the Data Controller to verify the accuracy, including the completeness, of the data, or

b) The Data Controller no longer needs them for the accomplishment of his or her tasks but they must be maintained for purposes of proof, or

c) The processing is unlawful and the data subject opposes their erasure and demands their blocking instead.

2. Requests for blocking shall specify the data to be blocked and the ground for the request.

3. If the ground for the request of blocking data is the inaccuracy of the data, as referred to in Article 11 (3), the Data Controller shall immediately block the data for the period necessary for verifying the accuracy and completeness of the data.

4. A data subject who has requested and obtained the blocking of data shall be informed thereof by the Data Controller. He or she shall also be informed of the fact that data are to be unblocked at least 15 working days before they are unblocked.

5. The Data Controller shall take a decision as soon as possible and at the latest within 15 working days of receiving a request for data to be blocked. If the request is accepted, it shall be acted upon within 30 working days and the data subject notified thereof. Should the request for blocking be rejected, the Data Controller shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the rejection.

6. In automated filing systems, blocking shall be ensured by technical means. The fact that personal data are blocked shall be indicated in the system in such a way as to make it clear that the data may not be used.

7. Personal data blocked pursuant to this Article shall, with the exception of their storage, only be processed for purposes of proof or with the consent of the data subject or for the purpose of protecting the rights of third parties.

Article 13
Right of erasure

1. The data subject shall have the right to obtain from the Data Controller the erasure of data if the processing thereof is unlawful.

2. Requests for erasure shall specify the data to be erased.

3. Where the Data Controller disputes that the processing is unlawful, he or she shall provide proof that it is lawful.

4. The Data Controller shall reply within 15 working days of receiving a request for erasure. If the request is accepted, it shall be acted upon immediately. If the Data Controller deems the request unjustified, he or she shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the decision.

5. Erasure entails the physical disappearance of the data without the necessity to replace them by a code or by the creation of an alternative file containing the data erased. If erasure proves impossible for technical reasons, the Data Controller shall block the data immediately. The data subject shall be duly informed of this procedure.

Article 14
Notification to third parties

The data subject shall have the right to obtain from the Data Controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking pursuant to Articles 11 to 13, unless this proves impossible or involves a disproportionate effort. In the event of a refusal to notify a third party on the grounds of impossibility or disproportionate effort, the Data Controller shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the refusal.

Article 15
Right to object

1. The data subject shall have the right to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in the cases covered by Article 5 (17)(b),(c) and (d) - in relation to Article 5(d) of the Regulation. For processing operations whose lawfulness is based on Article 5(d) of the Regulation, data subjects can withdraw their consent at any time.

2. The data subject shall have the right to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing and shall be expressly offered the right to object free of charge to such disclosure or use.

3. Requests to make an objection shall specify the date and the data concerned.

4. The Data Controller shall reply to the data subject within 15 working days of receiving a request to make an objection. If the Data Controller deems the request unjustified, he or she shall inform the data subject by means of a letter stating the grounds for the decision.

5. In the event of a justified objection the data in question may not be subjected to the processing referred to in Article 13(4).

Article 16
Monitoring procedure

1. Data Controllers concerned shall assist the Data Protection Officer in the performance of his or her duties and provide him or her with any information which he or she requests within 20 working days. In performing his or her duties, the Data Protection Officer shall have access at all times to the data being processed and to all offices, data processing installations and data carriers.

2. The Data Protection Officer may decide to carry out any other type of monitoring at any time in order to ensure that the Regulation is being correctly applied by eu-LISA.

Article 17
Remedies

1. Any person employed by eu-LISA may:

a) Lodge a complaint pursuant to Article 32(2) of the Regulation concerning complaints that can be filed by any data subject;

b) Lodge a complaint pursuant to Article 33 of the Regulation with the European Data Protection Supervisor alleging a breach of data protection rules, without being concerned as data subject themselves;

c) Lodge a request or a complaint pursuant to Article 90b of the Staff Regulations in respect of a matter relating to the processing of personal data. Lodging such a complaint does not have the effect of stopping time running for the purposes of lodging a complaint pursuant to Article 90 of the Staff Regulations.

2. If any person employed by eu-LISA lodges with the Appointing Authority a complaint pursuant to Article 90 of the Staff Regulations in respect of a matter relating to the processing of personal data, the Data Protection Officer shall be consulted.

Article 18
Restrictions

1. The Data Controller may restrict the rights laid down in Articles 10 to 14 of this Decision on the grounds set out in Article 20(1) of the Regulation. He or she shall consult the Data Protection Officer in advance.

2. If a restriction is imposed, the Data Controller shall, in accordance with Union law, inform the data subject of the principal reasons for the restriction and of his or her right to refer the matter to the European Data Protection Supervisor and the Court of Justice.

3. The Data Controller shall respond without delay to requests relating to the application of restrictions on the exercise of rights and shall give the reasons for any decision taken to that effect.

Article 19
Data controllers

1. By means of a specific decision, the Agency may appoint one or more data controller(s), within the meaning of Article 2(d) of the Regulation.

2. The data controller shall be responsible for ensuring that processing operations carried out under his or her supervision are in accordance with the Regulation. In particular, he or she shall be responsible for:

a) Assisting the Data Protection Officer and the European Data Protection Supervisor in the performance of their respective duties, in particular by sending information to them in reply to their requests within 20 working days at most;

b) Implementing appropriate technical and organisational measures and giving the members of eu-LISA staff (or other persons under their authority) suitable instructions for ensuring that processing is confidential and providing an appropriate level of security in view of the risks which processing entails; and

c) Notifying the Data Protection Officer of any data processing operation before undertaking it, pursuant to Article 6 of this Decision.

Article 20
Access to documents

The register of processing operations shall be public and accessible in electronic form. Any person may inspect it directly and request from the Data Protection Officer an authenticated copy of an entry pertaining to a specific processing operation. Indirect access shall also be possible via the European Data Protection Supervisor.

Article 21
Final provisions

This Decision shall enter into force immediately.

Done in Tallinn, 23.12.2013