European Aviation Safety Agency

DECISION NO 2010/140/E

OF THE EXECUTIVE DIRECTOR OF THE AGENCY

OF 30 SEPTEMBER 2010

ADOPTING IMPLEMENTING RULES CONCERNING DATA PROTECTION AT THE EUROPEAN AVIATION SAFETY AGENCY

THE EXECUTIVE DIRECTOR OF THE EUROPEAN AVIATION SAFETY AGENCY

- Having regard to Regulation (EC) N° 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 European Union institutions and bodies and on the free movement of such data, and in particular its article 24 (8) thereof;
- Having regard to Regulation (EC) 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing council directive 91/670/EEC, Regulation (EC) 1592/2002 and Directive 2004/36/EC, and notably Article 38.3(e) and 58.4 thereof ;

Whereas:

(1) Regulation (EC) 45/2001, hereinafter referred to as the “Regulation” sets out the principle and rules applicable to all Union institutions and bodies and provides for the appointment by each Union institution and Union 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 Union institution and body in accordance with the provisions in its Annex.

HAS DECIDED AS FOLLOWS:

SECTION ONE

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This decision lays down the rules and procedures for the implementation of the Regulation and its annex, within the European Aviation Safety Agency (EASA). It supplements the provisions in the Regulation relating to the Data Protection Officer's appointment and status, as well as to his or her tasks, duties and powers.
2. The Decision also clarifies the roles, tasks and duties of the Data Controllers, including the procedure for notifying a processing to the Data Protection Officer.
3. Furthermore, it lays down the rules according to which Data Subjects can exercise their rights and implements the procedure obtaining access to the Register of processing operations kept by the Data Protection Officer.

SECTION TWO

THE DATA PROTECTION OFFICER

Article 2

APPOINTMENT, STATUS AND INDEPENDENCE

1. The Executive Director shall appoint the Data Protection Officer and register him/her with the European Data Protection Supervisor.
2. The Data Protection Officer shall be selected on the basis of his or her personal and professional abilities and, in particular, his or her expert knowledge on data protection.
3. The term of the office for the Data Protection Officer shall be five years, with the possibility of renewal up to a maximum of ten years. He or she may be dismissed from his or her post only with the consent of the European Data Protection Supervisor and only if he/she no longer fulfils the conditions required for the performance of his or her duties. The European Data Protection Supervisor shall be consulted in writing and a copy of the letter shall be sent to the Data Protection Officer.
4. The Data Protection Officer may perform other duties, provided that they do not result in a conflict of interest with the role of the Data Protection Officer, particularly in relation to the application of the provisions laid down in the Regulation.
5. the Data Protection Officer shall maintain, including once he/she has ceased his or her duties, professional secrecy as regards any confidential

documents or information which he/she obtains in the course of his or her duties

6. The Data Protection Officer shall be independent in the performance of his or her duties[1]. He/she and may not receive instructions with respect to the performance of his/her duties[2].The Data Protection Officer shall refrain from any act which is incompatible with the nature of his or her duties.

Article 3

Tasks and Duties

1. With a view of ensuring that the provisions laid down by the Regulation are applied within European Aviation Safety Agency, the Data Protection Officer shall:

(a) Advise the Executive Director and the Data Controllers on matters concerning the application of data protection provisions within European Aviation Safety Agency

(b) Provide information to the European Aviation Safety Agency's Data Controllers and Data Subjects on their rights and obligations under the Regulation and facilitate the exercise of those rights and the fulfilment of those obligations.

(c) Keep a register of the data processing operations notified by the Data Controllers pursuant Article 26 of the Regulation and ensure that the register shall be inspected by any individual.

(d) Uphold Data Subject's rights and freedom by ensuring that the processing operation carried out in European Aviation Safety Agency do not undermine the freedom of the Data Subjects and ensure, in close cooperation with the Executive Director and the Data Controllers that no person suffers loss or damage for having brought to the attention of the Data Protection Officer a matter which in the view of that person constitutes an infringement to the Regulation

2. In relation to the European Data Protection Supervisor the Data Protection Officer shall:

(a) Cooperate with the European Data Protection Supervisor at latter's request or on the Data Protection Officer's own initiative within the Data Protection Officer's area of responsibilities, particularly regarding the dealing with complaints and carrying out inspections.

(b) Respond to request of the European Data Protection Supervisor.

(c) Notify to the European Data Protection Supervisor 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

[1] *Cf* Article 24.1.c Regulation (EC) 45/2001
[2] *Cf* Article 24.7 Regulation (EC) 45/2001

of a prior check, the Data Protection Officer shall consult the European Data Protection Supervisor.

3. The Data Protection Officer may be consulted at any time by the Executive Director, any Data Controllers concerned, the Staff Committee and in particular by Data Subjects, without going to official channels, in respect of any matter relating to the interpretation or application of the Regulation

4. The Data Protection Officer shall represent The European Aviation Safety Agency in any matter – excluding court cases- relating to the protection of personal data. He or she may in particular attend meetings of committees or bodies at international level.

Article 4

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 Controllers or to the Executive Director on issues concerning the application of the Regulation or included in these implementing rules.

(b) Consider issues and facts (on his or her own initiative or at the request of the Data Controllers, the 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 right of the Data Subject. The Data Protection Officer shall forward his or her findings to the person who submitted the request and to the Data Controller.

(c) Request clarifications from any European Aviation Safety Agency Directorate, Department or Section on any matter related to Data Protection Officers tasks and duties.

(d) Issue an opinion (on his or her own initiative) on the lawfulness of actual or proposed data processing operations and on the measures required in order to ensure that such operations are lawful and on the suitability or inadequacy of data or security measures. The opinion may in particular relate to any issue concerning the notification of data processing.

(e) Report any breach of the provision laid down in the Regulation to the Executive Director.

(f) Regularly attend meeting with the European Data Protection Supervisor and or the Data Protection Officers of the other Union institutions and bodies with a view to establishing a mutual exchange of information, engaging interinstitutional cooperation and harmonising the application of the procedures in force.

(g) Drawn up an annual activity report for the Executive Director and the European Data Protection Supervisor concerning activities relating to the protection of data within European Aviation Safety Agency. He/she shall make the report available to all European Aviation Safety Agency staff.

2. The Data Protection Officer shall have access at all times to all type of data which are being processed and to all offices, data processing installations and data carriers.

3. The Data Protection Officer may decide to carry out monitoring of the procedure at any time, in order to ensure that the Regulation is being applied by the European Aviation Safety Agency.

Article 5

Support to the Data Protection Officer

Any staff providing support to the Data Protection Officer in relation to data protection issues shall act solely on the Data Protection Officer's instructions and shall be bound by the same duty of professional secrecy as the Data Protection Officer as regards any confidential documents or information which they obtain in the course of their duties.

SECTION THREE

THE DATA CONTROLLERS

Article 6

Appointment, tasks and duties

1. By means of a specific decision, the Executive Director may appoint an authority subordinate to him or her as Data Controller, within the meaning of Article 2 (d) of the Regulation.

2. The Data Controller shall ensure that all processing operations involving personal data that are performed within their area of responsibility comply with the Regulation. To this end, the Data Controller shall:

(a) Implement appropriate technical and organisational measures and give the European Aviation Safety Agency's staff members (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 the processing entails.

(b) Notify without delay to the Data Protection Officer any data processing operation before undertaking it, pursuant to article 25 of the Regulation and following the notification procedure set out in article 7 of the present Decision. The Data Controllers should notify to the Data Protection Officer the already existing procedure within one year form the entry into force of this Decision.

(c) Assist the Data Protection Officer and the European Data Protection Supervisor in the performance of their tasks and, in particular, provide full information to them, grant access to the personal data and respond to questions within 20 working days of the receipt of the request.

3. In particular the relevant Data Controllers shall ensure that the Data Protection Officer is kept informed without delay:

(a) When an issue arises that has, or might have, data protection implications; and

(b) In respect of all contacts with external parties relating to the application of the Regulation, notably any interaction with the European Data Protection Supervisor.

Article 7

Notification Procedure

1. Each Data Controller shall notify, using the dedicated template:

(a) Any new processing operations relating to personal data before introducing them, and

(b) Any data processing operations already in place at the moment of the entry into force of the present Decision.

The notification shall include the information referred to in point 1 of the Annex and shall be sent to the Data Protection Officer through internal mail.

2. The relevant Data Controller shall notify any processing operation likely to present specific risks as listed in point 2 of the annex which is subject to prior checking by the European Data Protection Supervisor sufficiently well in advance of its implementation, to allow for the prior checking.

3. The Data Controller shall immediately inform the Data Protection Officer of any change affecting the information contained in a notification already submitted to the Data Protection Officer.

SECTION FOUR

REGISTER OF PROCESSING OPERATIONS

Article 8

Register

1. The Data Protection Officer shall keep a Register of the data processing operation notified pursuant Article 7 (1). The register shall detail all the notified data processing operations which are carried out at the European Aviation Safety Agency and shall indicate in particular the department responsible for the processing, the data processed and the intended purposes.

2. The register shall contain at least the information refereed to in point 1.1 to 1.7 of the Annex.

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.

4. The register shall be public, in paper and electronic form, and may be inspected by any person. Data Subject may make use of the information contained in the Register to exercise their rights under Articles 13 to 19 of the Regulation.

SECTION FIVE

DATA SUBJECTS' RIGHTS

Article 9

General Rules Governing the Exercise of rights by the 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.

2. Requests to exercise one of those rights shall be addressed to the Data Controller. Data Subjects who are EASA staff members may use a dedicated form which shall be available in electronic form on European Aviation Safety Agency's Intranet. The request shall contain:

- The name, first name and contact details of the Data Subject;
- An indication of the right to be exercised;
- Where appropriate, supporting documents relating to the request;
- The category or categories of data concerned;
- The applicant's signature and the date of the request

The request may be submitted 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 error or omissions, the Data Controller may ask for additional information. The Data Controller shall verify the applicant's credentials.

3. The Data Controller shall respond to any request to exercise the rights. An acknowledgment 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 acknowledgment 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.

4. The Data Controller shall notify the Data Subject of his or her rights to lodge a complaint with the European Data Protection Supervisor if that

person considers that the rights granted to him or her under Article 16 of the Treaty were infringed when his or her personal data were processed.

5. The Data Subject may exercise any of these rights free of charge.

6. Request to exercise a right may be rejected in the cases referred to in Article 20 of the Regulation, subject to application of Article 20 (Remedies) of this Decision.

Article 10

Right of Access

1. The Data Subject shall have the right to obtain at any time within three months from the receipt of the request form 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;

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;

(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 form 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 the request may be accompanied by supporting documents.

3. If a request for rectification is accepted, it shall be acted upon without delay and the Data Subject notified thereof. Should a request for rectification be rejected, the Data Controller shall have 15 working days to inform the Data Subject by means of a letter stating the ground 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 the purposes of evidence, 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. A Data Subject who has requested and obtained the blocking of data shall be informed thereof by the Data Controller. The controller shall inform the Data Subject who made the request before the data are unblocked.

Article 13

Right of Erasure

1 The Data Subject may request the controller to erase data without delay in case of unlawful processing, particularly where the provisions of Articles 4 to 10 of the Regulation have been infringed.

2. The request shall specify the data concerned and shall provide the reasons or evidence of the unlawfulness of the processing. In automated filing systems, erasure shall in principle be ensured by all appropriate technical means, excluding the possibility of any further processing of the erased data. If erasure is not possible for technical reasons, the controller, after consultation of the DPO, shall proceed to the blocking of such data without delay. The Data Subject shall be duly informed of this procedure.

3. The Data Controller shall reply within 15 working days of receiving a request for erasure. If the request is accepted it shall be acted without delay. If the Data Controller deems the request unjustified, he or she shall have 15 working days to inform the Data Subject by means of a letter stating the grounds for the decision.

Article 14

Notification to third parties[3]

1 In case of any rectification, blocking or erasure following a request made by the Data Subject, he/she may obtain from the controller the notification to third parties to whom his or her personal data have been disclosed, unless

[3] *Cf* Article 17 Regulation (EC) 45/2001

this proves impossible or involves a disproportionate effort. In the event of a refusal to notify a third party on the ground of impossibility or disproportionate effort, the Data Controller shall have 15 working days 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 (b), (c) and (d) of the Regulation.
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 expressively offered the right to object free of charge to such disclosure or use.
3. Requests to make an objection shall specify 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 informed 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 paragraph 1.

Article 16

Automated individual decision[4]

1. The Data Subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or Union legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the Data Subject's legitimate interest, such as arrangement allowing him or her to express his or her point of view, must be taken.

Article 17

Recourse to the Data Protection Officer

[4] *Cf* Article 19 Regulation (EC) 45/2001

1. Data Subject may contact the Data Protection Officer in the event that the Data Controller does not respect the relevant time limits set out in article 10 to 15.
2. In the event of abuse by the Data Subject in exercising his or her rights, the Data Controller may refer the matter to the Data Protection Officer. In this case the Data Protection Officer shall decide on the merit of the request and on the appropriate follow-up.
3. In the event of disagreement between the Data Subject and the Data Controller, both parties shall have the right to consult the Data Protection Officer

Article 18

Restrictions

1. The Data Controller may restrict the rights laid down in Article 10 to 14 of these Implementing Rules 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 the European Union law, inform the Data Subject of the principal reasons for this restriction and of his or her right to refer the matter to the European Data Protection Supervisor.
3. The Data Controller shall respond without delay to requests relating to the application of restrictions on the exercise of rights and shall give reasons for any decision taken to that effect.

Article 19

Investigation procedure

1. Any request for an investigation under Article 4(1)(c) by the Executive Director, a Data Controller, the Staff Committee or any individual, shall be addressed to the Data Protection Officer in writing.
2. The Data Protection Officer shall send an acknowledgment of receipt to the requester within five working days of the receipt of the request.
3. The Data Protection Officer may investigate the matter on site and request a written statement form the Data Controller. The Data Controller shall provide a response to the Data Protection Officer within 20 working days upon receipt of the Data Protection Officer request. The Data Protection Officer may ask for additional information or assistance from any European Aviation Safety Agency's Department. The relevant department shall provide such additional information or assistance within 20 working days of the Data Protection Officer's request.
4. The Data Protection Officer shall report back to the requester within three calendar months of receipt of the request. If the Data Protection Officer

deems it appropriate, he or she may inform all other parties concerned accordingly.

Article 20

Remedies

1. In addition to the remedies laid down by Article 32 of the regulation, which are available to any Data Subject, any person employed by the European Aviation Safety Agency may lodge a complaint pursuant Article 33 of the Regulation with the European Data Protection Supervisor. The European Aviation Safety Agency' employees are recommended to contact the Data Protection Officer in advance of lodging a complaint. Lodging such a complaint shall not have the effect of stopping time running for the purposes of lodging a complaint pursuant to article 90 of the Staff Regulations.
2. Irrespective of the right referred to in paragraph 1, any person employed by the European Aviation Safety Agency may lodge with the Appointing Authority a complaint pursuant Article 90 of the Staff Regulations in respect to a matter relating to the processing of personal data. In that case, the Data Protection Officer shall be consulted.

SECTION SIX

Article 21

Entry into Force

The present decision shall enter into force on the date of signature. It shall be published in the Agency's Official Publication.

Done at Cologne, 30 September 2010

P. GOUDOU

ANNEX

1. Notification procedure to the Data Protection Officer as referred to in article 7 (1)

The information to be given in the notification shall include:

1.1 The name and address of the data Controller and an indication of the organisational parts of an institution or body entrusted with the processing of personal data for a particular purpose;

1.2 The purpose or purposes of the processing;

1.3 A description of the category or categories of Data Subjects and of the data or categories of data relating to them;

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

1.5 The recipients or categories of recipients to whom the data might be disclosed;

1.6 A general indication of the time limit for blocking and erase the different categories of data;

1.7 Proposed transfers of data to third countries or international organisations;

1.8 A general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 of the Regulation to ensure security of the processing.

2. Processing operations subject to prior check as referred to in Article 7 (2)

The following processing operations are likely to present specific risks to the rights and freedoms of the Data Subjects by virtue of their nature, their scope or their purposes:

2.1 processing of data relating to health and suspected offences, offences, criminal convictions or security measures (e.g. medical files and infringement reports);

2.2 Processing operations intended to evaluate personal aspects relating to the Data Subject, including his or her ability, efficiency and conduct (e.g. probationary period reports, performance appraisal)

2.3 Processing operation allowing linkages not provided for pursuant to national or Union legislation between data processed for different purposes.