NOTE DE SERVICE/OFFICE NOTICE

EUROCONTROL

Numéro/Number: **25/17** Date : **25/10/17**

Implementing Rules concerning the EUROCONTROL Regulation on Personal Data Protection

Attachment: Implementing Rules concerning the EUROCONTROL Regulation on Personal Data Protection

1. INTRODUCTION

The *EUROCONTROL Regulation on Personal Data Protection,* approved by the Permanent Commission on 28.12.2006 and published by Office Notice 34/08 of 2.7.2008, defines the basic conditions for the processing and protection of personal data by the Organisation.

It is necessary to publish *Implementing Rules concerning the EUROCONTROL Regulation on Personal Data Protection* in order to clarify certain aspects of the Regulation and deal with issues which are not addressed in the Regulation, in particular:

- the roles and tasks of the actors of the data protection system (Data Protection Officer, data controllers, processors and data protection coordinators);
- the conditions for the transmission of personal data within the Organisation and to recipients outside the Organisation;
- the modalities for the exercise of rights of the persons whose data are processed ("data subjects").

The provisions of the new Rule can be found in the **Attachment**.

2. KEY ELEMENTS OF THE IMPLEMENTING RULES

2.1. Actors

It is the obligation of the managers responsible for the processing of personal data to ensure the correct application of the data protection requirements. The Rules define the obligations of the so-called personal **data controllers** (Article 3). Any data controller shall in particular keep an inventory of the personal data processing systems under their authority. They shall further inform the Data Protection Officer timely about any projects concerning the processing of personal data by automatic means.

Directors are, where they have not done so, called upon to designate a **data protection coordinator** (Article 4) who assists the data controllers in their tasks and facilitates the exchange of information with the Data Protection Officer.

The data controller does not always carry out the processing himself/herself, in particular in the case of IT systems. Where the data controller uses a **processor** (e.g. the Agency's IT services or a contractor), the data controller remains responsible for compliance. The processor must establish adequate security measures (Article 5). If the processing is outsourced, the contract with the external company must include certain elements mentioned in the Annex to the Rules.

2.2. Transmission of personal data

As a general rule personal data may only be transmitted to recipients if the data are necessary for the legitimate performance of tasks covered by the recipient's competence (Article 6).

The Regulation allows **transmission of personal data outside EUROCONTROL** only for the purposes of the Organisation. An exception is the transmission of personal data to authorities (courts of law, national police forces, tax and customs authorities and investigative bodies) in the framework of an inquiry.

The Rules define the conditions and safeguards for the transmission of data to third parties (Articles 7 and 8). Essentially, transmission is admissible only if the recipient provides an adequate level of protection.

The Rules create a presumption for the existence of an adequate level of protection in the case of recipients:

- located in States which have ratified Council of Europe Convention No. 108 on data protection (all 41 EUROCONTROL Member States have done so); and
- which are EU institutions subject to *Regulation (EC) 45/2001* on the protection of personal data.

2.3. Exercise of the rights of data subjects

The Regulation grants each data subject the following rights:

- to know about the data processing;
- access to all data concerning him/her;
- the right of rectification, erasure or blocking of data;
- and the right to request the DPO to make an investigation.

The Regulation however makes no reference to the formal/procedural aspects of such rights and these are therefore provided by the Rules.

EUROCONTROL

3. ADDITIONAL INFORMATION

The Data Protection Officer has developed guidance material for persons who are responsible for personal data processing in the Agency in order to assist them with the implementation of their obligations. Please visit the webpage of the Data Protection Officer on MyOrbite: https://intra.eurocontrol.int/dg/jur/public/standard_page/protection_of_personal_data.html. They may also apply to the Data Protection Officer for training.

4. ENTRY INTO FORCE

The provisions of the Implementing Rules *concerning the EUROCONTROL Regulation on Personal Data Protection* will enter into force as from the date of publication of the present Office Notice.

Frank BRENNER

Attachment

Implementing Rules concerning the EUROCONTROL Regulation on Personal Data Protection (Office Notice 34/08 of 2 July 2008)

Having regard to Article 3 of the Statute of the Agency;

Having regard to the EUROCONTROL Regulation on Personal Data Protection, and in particular its Articles 6.2, 8.4 and 10;

The Director General has adopted the following implementing rules for the implementation of the EUROCONTROL Regulation on Personal Data Protection, (Office Notice 34/08 of 2.7.2008):

Section 1
General provisions

Article 1 – Definitions

(a) "EUROCONTROL Convention" shall mean the International Convention relating to Co-operation for the Safety of Air Navigation of 13 December 1960 as amended by the Protocol signed at Brussels on 12 February 1981 and revised by the Protocol of 27 June 1997;

(b) "Regulation" shall mean the EUROCONTROL Regulation on Personal Data Protection as approved by Measure No. 06/129 dated 28.12.2006 of the Permanent Commission and published by Office Notice 34/08 dated 2.7.2008;

(c) "data controller" shall mean the person responsible for the organizational unit that determines the purposes and means of the processing of personal data carried out under his or her authority;

(d) "processor" shall mean a natural or legal person or any other body or organizational unit which is authorized to process personal data on behalf of the data controller;

(e) "data subject" shall mean the identified or identifiable natural person referred to in Article 2 (a) of the Regulation whose personal data is processed by the Organisation;

(f) "recipient", "personal data", "processing of personal data", "data subject's consent", "filing system" and "third party" shall have the meaning defined in Article 2 of the Regulation;

(g) "data protection register" shall mean a repository in electronic format which shall contain all personal data filing systems and processing programmes in accordance with Article 8.3 of the Regulation;

(h) "programme for processing personal data" ("processing programme"): shall mean any automated application designed or used for the processing of personal data even if the processing of personal data is only ancillary to its main purpose;

(i) "blocking" shall mean the freezing of data by the data controller in a given moment for a specific period of time by appropriate technical means which make clear that the personal data concerned may not be used unless they are necessary for purposes of proof or in order to protect the rights of a third party.

Section 2
Roles and actors

Article 2 – Data Protection Officer

1. The term of office of the Data Protection Officer (DPO) shall be five years, renewable for further periods of equal length. Without prejudice to the relevant provisions of the Regulation, the DPO shall be subject to the service regulations applicable to officials or servants of EUROCONTROL. The DPO may be assisted in the exercise of his/her function.

2. Without prejudice to other tasks and powers under the Regulation and the present implementing rules, the Data Protection Officer may on his/her own initiative or on the initiative of the Director General, the Internal Audit, or any interested individual, make queries on any matters and occurrences directly related to his/her tasks. He/she invites the person responsible to comment within a period which he/she shall specify. He/she may bring to the attention of the relevant manager or the Director General any shortcomings or failure to comply with the obligations of the Regulation and the present implementing rules and make relevant recommendations.

3. The Data Protection Officer shall receive information in reply to his queries and have access to the information necessary for the performance of his tasks, in particular to the data which are the subject of the processing and to all data processing installations and data carriers.

Article 3 – Data controllers

1. Data controllers are responsible for ensuring that the processing operations carried out under their authority comply with the Regulation and the present implementing rules. They shall take the necessary measures in this regard.

2. In particular, data controllers shall

   (a) keep the Data Protection Officer timely informed about any projects concerning the processing of personal data by automatic means;

   (b) where appropriate, consult the Data Protection Officer on the conformity of the processing of personal data;

   (c) keep an inventory of all filing systems and programmes for processing of personal data under their authority;

   (d) notify to the Data Protection Officer for inclusion in the data protection register at least the particulars mentioned in Article 8.3 of the Regulation in respect of all filing systems and processing programmes under their authority.

3. Data controllers may delegate their tasks to other persons acting under their authority.

Article 4 – Data protection coordinators

1. A data protection coordinator shall be designated for each Directorate or site of the Agency among the members of the staff of the Agency, preferably the HR Business Partners, by the Directors in consultation with the Data Protection Officer.

2. Without prejudice to the responsibilities of the Data Protection Officer, the data protection coordinator shall:

   (a) assist the data controllers in complying with their obligations and coordinate the implementation of the Regulation and the present implementing rules in the Directorate or site;

(b) facilitate the exchange of information between the data controllers and the Data Protection Officer.

Article 5 – Processing of personal data on behalf of data controllers

1. Where data processing is carried out on behalf of a data controller, the data controller shall designate a processor which provides sufficient guarantees in respect of the technical and organisational security measures required by Article 7 of the Regulation. The data controller remains responsible for compliance with those measures.

2. Processors within the Agency shall act on the data controllers' instructions and in strict compliance with the provisions of the Regulation and the present implementing rules. Personnel of the processor which is not staff of the Agency shall be required to sign a confidentiality agreement.

3. The processing of personal data by a processor outside of the Agency shall be governed by a written contract or legal act binding the processor, which shall include the elements set out in the Annex.

   The provisions of Article 7 of the present implementing rules concerning the requirement of an adequate level of protection in the country or legal system of the processor shall apply.

Section 3
Transmission of personal data

Article 6 – Transmission of personal data to recipients within EUROCONTROL

1. Without prejudice to Articles 3 to 5 of the Regulation, personal data shall only be transmitted to recipients within the Organisation if the data are necessary for the legitimate performance of tasks covered by their competence.

2. The data controller shall verify the competence of the recipient and make a prima facie evaluation of the necessity of the transmission. In the case of doubt concerning the necessity of the transmission, the data controller shall request the recipient to credibly show its necessity. The recipient shall ensure that the necessity of the transmission can be subsequently verified.

3. The recipient shall process the personal data only for the purposes for which they were transmitted.

Article 7 – Transmission of personal data to recipients outside EUROCONTROL

1. Without prejudice to Articles 3 to 6 of the Regulation, personal data shall only be transmitted to recipients outside the Organisation to allow tasks covered by the competence of the Organisation (Article 3 of the Regulation) to be carried out or under the conditions specified by the data controller and provided that an adequate level of protection is ensured in the country or legal system of the recipient.

2. The data controller shall make an assessment whether the recipient affords an adequate level of protection by taking into consideration all relevant circumstances surrounding the transmission of the data, including:

   - the nature and the sensitivity of the data;
   - the purpose and the duration of the processing by the recipient;
   - the recipient and the country in which the recipient is located;
   - the applicable rules of law to which the recipient is subject;

– the confidentiality and security measures applied by the recipient.

3. An adequate level of protection is considered to be ensured in the case of transmissions:

   a) to recipients established in States which have ratified the *Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* of the Council of Europe signed on 28.1.1981;

   b) to institutions or bodies of the European Union insofar as the processing of the transmitted data by the institution or body is subject to *Regulation (EC) 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.*

4. In cases of doubt, the Director General decides on the adequacy of the protection ensured in the country or the legal system of the recipient.

5. By way of derogation from paragraphs 1 and 2 (no adequate level of protection is ensured in the country where the recipient authority is located), personal data may be transmitted if:

   a) the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

   b) the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the data controller and a third party; or

   c) the transmission is necessary in order to protect the vital interests of the data subject; or

   d) the transmission is made from a register which according to EUROCONTROL regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for consultation are fulfilled in the particular case; or

   e) the data subject has unambiguously given his or her consent.

6. Furthermore, the Director General may authorise transfers of personal data to recipients who do not ensure an adequate level of protection within the meaning of this Article, where the data controller provides adequate safeguards with respect to the protection of personal data and the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses or other binding legal acts.

7. The data controller shall bind the recipient, where possible, in accordance with Article 6.1 (a), (b) and (c) of the Regulation:

   (a) to obtain the prior consent of the Organisation for any further transmission of the data;

   (b) to process the data transmitted in pursuance of this Article only for the purposes set out in Article 3 of the Regulation or under the conditions specified by the data controller; and

   (c) to inform the transmitting body of the measures taken to protect the transmitted data in compliance with the purposes and conditions specified by it at the time of the transmission.

8. The present Article is without prejudice to any rules applicable to the protection of specific types of personal data[1].

[1] E.g. rules governing incident and accident reporting obligations and 'just culture'

Article 8 – Transmission of personal data to authorities in the framework of an inquiry

1. The transmission of data to authorities in the framework of a particular inquiry covered by the competence of that authority is authorised if the recipient authority establishes that the data are necessary for the performance of a task carried out in the public interest or in the exercise of public authority and provided that an adequate level of protection is ensured in the country or legal system of the recipient authority. Paragraphs 2, 3 and 4 of Article 7 shall apply.

2. By way of derogation from paragraph 1 of this Article (no adequate level of protection is ensured in the country where the recipient authority is located), the Director General may authorise the transmission of personal data to authorities in the framework of a particular inquiry covered by the competence of that authority if:

   a) the transmission is necessary or legally required on important public interest grounds; or

   b) the transmission is necessary for the protection against serious threats to public security and public order; or

   c) the transmission is necessary for the prosecution of criminal offences; or

   d) the transmission is necessary in the framework of judicial proceedings, or for the establishment or exercise of, or defence against, legal claims; or

   e) the transmission is necessary to protect the vital interests of the data subject.

   In making a decision, the Director General shall take into account the principle of proportionality and the legitimate interests of the person concerned.

3. For the purpose of this Article authorities are courts of law and law-enforcement authorities, including local and national police forces, tax and customs authorities and investigative bodies.

4. The present Article is without prejudice to any rules applicable to the protection of specific types of personal data[1].

Section 4
Duty of information

Article 9 – Information to be provided to the data subjects

1. The data controller shall inform the data subject without delay about at least the following details of the processing of his/her personal data unless he/she already has them:

   a) the identity of the data controller;

   b) the purposes of the processing;

   c) the categories of data concerned;

   d) the recipients or categories of recipients of the data to the extent that transmission is not to be expected taking into account the circumstances;

   e) the data subject's rights of access and rectification.

2. Where the data is collected from the staff of the Agency, the obligation to inform the data subject may be achieved by an appropriate reference to the data protection register.

3. The application of paragraph 1 of this Article may be restricted in the case of compelling reasons of confidentiality or in the public interest or if informing the data subject would be impossible or require a disproportionate effort.

Section 5
Rights of data subjects

Article 10 – Rights of data subjects

1. Requests for the exercise of the data subject's rights provided for in Article 9 of the Regulation shall be addressed by the data subject in writing to the data controller indicating the data concerned and the reasons for their request. The requester's identity must be verified by the data controller.

2. Where the data subject has made a request for access to personal data, the data subject has the right to obtain within three months from the receipt of the request:

   (a) confirmation as to whether personal data relating to him are processed and, if so, communication of these data to him in an intelligible form, including information concerning their source where the data have not been collected from the data subject;

   (b) information concerning the purposes, the legal basis of processing and the recipients or categories of recipients to whom such data are disclosed.

   Article 9, paragraph 3 shall apply mutatis mutandis.

3. At the data subject's request, the data controller shall rectify without delay incorrect or incomplete personal data and shall notify the third parties to whom the data have already been transmitted of any rectification of data, unless this proves to be impossible or requires undue effort.

4. Where the data subject has made a request for erasure of personal data, the data controller shall erase by a reasonable deadline any data the processing of which does not comply with the Regulation. For the purpose of this Article, "erasure" shall mean the obliteration of stored data in such a way that reconstruction is not possible (physical erasure) as well as the permanent prevention of access to data by programming measures (logical erasure).

5. The data controller shall block personal data if:

   a) data processed by automated means are to be erased and for technical reasons the erasure is not possible or if the data have to be maintained for the purposes of proof;

   b) the processing does not comply with the Regulation and the data subject demands their blocking instead of erasure;

   c) their accuracy is contested by the data subject. In this case the data shall be blocked for a period enabling the data controller to take a final decision.

   The data subject shall be informed before the data are unblocked.

6. In the event of obvious abuse by a data subject in exercising his/her rights, the data controller may refer the data subject to the Data Protection Officer. In such case, the Data Protection Officer will decide on the merits of the request and the appropriate follow-up.

7. If requests for access cannot be fulfilled within three months, the Data Protection Officer may extend this time limit at the data controller's request. Any such extension shall be notified to the requester.

Section 6
Investigations

Article 11 – Investigations pursuant to Article 10.1 of the Regulation

1. Applications by a data subject for an investigation pursuant to Article 10.1 of the Regulation shall be made in writing to the Data Protection Officer. Within two weeks of receipt, the Data Protection Officer shall send an acknowledgement of receipt to the applicant. The Data Protection Officer shall determine in consultation with the applicant whether the request is to be treated as confidential.

2. The Data Protection Officer shall request a written statement from the data controller who is responsible for the data processing operation in question. The data controller shall provide his/her response within three weeks. The Data Protection Officer may request complementary information from the data controller or other parties which shall be provided within three weeks. Depending on the complexity of the case and the expertise needed, the Data Protection Officer may request the necessary assistance from the Agency Security Officer, or from experts outside the Agency.

3. The Data Protection Officer shall report to the applicant no later than three months following receipt of the request. This period may be suspended until the Data Protection Officer has received any further information that he/she may have requested pursuant to paragraph 2 of this Article. If deemed appropriate, all other parties concerned should be informed accordingly.

Section 7
Data protection register

Article 12 – Data protection register

1. The data protection register shall be kept in electronic form on the basis of notifications received from the data controllers.

2. The register may be inspected by any staff of the Organisation. Persons other than staff of the Organisation may inspect entries in the register related to the categories of data subjects to which they belong.

-.-.-

Annex

Elements to be included in the contract or legal act with the external processor

1. General requirements

As regards Article 5.3 of the present Rules, the written contact or legal act binding the processor shall provide that the processor shall:

(a) act only on instructions from the data controller documented in writing;

(b) keep the data confidential;

(c) ensure compliance with the principles set out in Article 4 of the Regulation;

(d) ensure compliance with the technical and organisational security measures required by Article 7 of the Regulation.

2. Specific requirements

In particular, the contract or legal act binding the processor shall include:

(a) the subject and duration of the work to be carried out;

(b) the extent, type and purpose of the intended data processing;

(c) the rectification, erasure and blocking of data;

(d) any right to issue subcontracts;

(e) the data controller's rights to monitor and the processor's corresponding obligations to accept and cooperate;

(f) the duty of the processor to employ only staff who have committed themselves to confidentiality;

(g) the duty of the processor to notify the data controller of any breach of data protection provisions, and

(h) the return of data storage media and/or the erasure of data recorded by the processor after the work has been carried out.