

Athena Data Protection implementing rules

Approved by the Athena Special Committee on March 9, 2016

Having regard to COUNCIL DECISION (CFSP) 2015/528 of 27 March 2015 establishing a mechanism to administer the financing of the common costs of European Union operations having military or defence implications (Athena) and repealing Decision 2011/871/CFSP and in particular Article 46,

Having regard that said Article 46 provides that Athena shall protect individuals with regard to the processing of their personal data in accordance with the principles and procedures laid down in Regulation (EC) No 45/2001 of the European Parliament and of the Council.

The Athena Special Committee adopts the following implementing rules as regards the application of Regulation 45/2001 to Athena:

1 - Scope

Without prejudice of the application of Regulation 45/2001 to the administrator, the accounting officer and any EU official or other servant of the Union, the present Athena Data Protection implementing rules shall apply to all actions and tasks undertaken on behalf of Athena mechanism, in particular by:

- any staff made available to Athena by Member States;
- any meetings of the Special Committee and any documents or proceedings thereof;
- any actions or tasks carried out by the operation commander on behalf of Athena under Article 8 of Council Decision (CFSP)2015/528;
- any arrangements or framework contracts entered into with Member States, EU institutions and bodies, third States and International Organizations.

2 – Definitions

For the purposes of these implementing rules:

(a) **'personal data'** shall mean any information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

(b) **'processing of personal data'** hereinafter referred to as 'processing' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) **'controller'** shall mean Athena, represented by the Special Committee, the administrator or the commander of each operation as the case may be

(d) **'processor'** shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(e) **'third party'** shall mean a natural or legal person, public authority, agency or body other than the data subject, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;

(f) **'recipient'** shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

3 - Purpose, data quality and proportionality

The controller will ensure that personal data is:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

4 – Legal basis for processing personal data

Personal data should only be processed based on one the following grounds:

- processing is necessary for the performance of the tasks entrusted to Athena; or
- processing is necessary for compliance with a legal obligation to which Athena is subject; or
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- the data subject has unambiguously given his consent; or
- processing is necessary in order to protect the vital interests of the data subject.

5 - The processing of special categories of data

5.1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited.

5.2. Paragraph 5.1 shall not apply where:

- a) the data subject has given his or her express consent to the processing of those data, or
- b) processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law, subject to adequate safeguards, or
- c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent, or
- d) processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

5.3. Paragraph 5.1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

6– Transparency and information rights

6.1. The administrator shall provide data subjects, through the Athena Web page or through any other specific channel deemed appropriate, with the following information:

- (a) the identity of the controller;
- (b) the purposes of the processing operation for which the data are intended;
- (c) the recipients or categories of recipients of the data;

(d) the existence of the right of access to, and the right to rectify, the data concerning him or her; and

(e) any further information such as:

(i) the legal basis of the processing operation for which the data are intended,

(ii) the time-limits for storing the data.

6.2. In addition, where the data have been obtained from the data subject, he/she should be informed whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;

6.3. Where data is not collected from the data subject, he/she should be informed of the categories of data being collected.

7 – Rights of access, rectification, erasure and blocking of data:

7.1. The data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the 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;

7.2. The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.

7.3. The data subject shall have the right to obtain from the controller the blocking of data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the data, or;

(b) Athena no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof, or;

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

7.4. Personal data blocked pursuant to paragraph (c) shall, with the exception of their storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of a third party.

7.5. The data subject shall have the right to obtain from the controller the erasure of data if their processing is contrary to these implementing rules in particular where the provisions of Rules 3, 4 and 5 have been infringed.

7.6. The data subject shall have the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking pursuant to this rule unless this proves impossible or involves a disproportionate effort.

7.7. 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. Where there is a justified objection, the processing in question may no longer involve those data;

7.8. 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.

8 –Procedures for data subjects to exercise their rights

8.1. Any request to exercise rights shall be addressed by the individual concerned to the controller.

8.2. An acknowledgement of receipt will be sent within five working days. Access to data should be given within 3 months of receiving the request. Reply to any request of rectification, blocking or erasure shall be sent no later than 15 working days of the date of receipt of that request.

8.3. The deadline for the correction, block or deletion of data may not exceed 10 working days, with the period starting only from the date the decision is taken on the request to block or erase data.

9 – Exemptions and restrictions

The controller may restrict the application of rules 6,7 and 8 where such restriction constitutes a necessary measure to safeguard:

- (a) the prevention, investigation, detection and prosecution of criminal offences;
- (b) an important economic or financial interest of Athena, its mission or of a participating Member State,
- (c) the protection of the data subject or of the rights and freedoms of others;
- (d) the security, public security or defence of Athena mission or of a participating Member States;
- (e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b).

10 - Security of processing

Having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful

destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.

11 – Relationships with processors

11.1. Where a processing operation on behalf of Athena is carried out by a third party the controller must choose a processor providing sufficient guarantees in respect of the technical security and organizational measures governing the processing in accordance with rule 10 above.

11.2. The controller shall instruct the processor by written contractual means, among others:

- a) That the processor shall act only on instructions from the controller in what concerns handling of personal data,
- b) The rules relating to the security and confidentiality to be incumbent on the processor.

12 –Transfers to external parties

11.1. The controller shall transfer personal data to third parties only if the data are necessary for the legitimate performance of legitimated tasks covered by the competence of the recipient.

11.2. In addition to the requirements of paragraph 11.1, the transfer of personal data to recipients other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, or to any subsequent legal provision replacing said Directive, shall only be carried out by the controller if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation.

13 – Compliance and supervision of compliance

13.1. Athena appoints the Data Protection Officer of the Council as Data Protection Officer (DPO) of Athena operations with the tasks of ensuring in an independent manner the internal application by Athena of these implementing rules. The Data Protection Officer shall have in relation to Athena similar tasks and powers as those conferred upon him/her by Council Decision 2004/644/EC of 13 September 2004 as regards the Council.

13.2. The DPO shall:

(a) ensure in an independent manner the internal application of the provisions of the Athena Data Protection implementing rules. To this end, the DPO shall give advice to and be consulted by Athena management and make recommendations for the practical improvement of data protection by Athena. the DPO shall be informed by Athena management of any request to exercise rights by a data subject and of any complaint received.

(b) ensure that all Athena staff are informed of their rights and obligations pursuant to the Athena Data Protection implementing rules. The DPO shall in data protection issues and may be consulted by any Athena staff or any person dealing with Athena.

(c) ensure that the controller keeps the necessary documentation in relation to the processing operations; The DPO shall have access to any information or data to monitor that the controller is complying with its obligations under the Athena Data protection implementing rules.

(d) thus, ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations. To this end the DPO may be consulted by any person concerned.

14 – Updates of these implementing rules

14.1. The present implementing rules will be reviewed within 6 months from the adoption of any amendments to Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000.

14.2. Likewise, they will be reviewed within 6 months of the adoption of any amendment to Council Decision (CFSP) 2015/528.

14.3. Any substantial modifications of the present implementing rules shall be communicated to data subjects in accordance with rule 6 above.

15 – Relationship between national laws and the present implementing rules

If a national law is also applicable to any of the processings under the scope of the present implementing rules, such processing should comply with the said national rules, without prejudice to the obligations imposed by these implementing rules.