European Union Aviation Safety Agency

FO Personal data processing records and compliance checklist - Public	Ref # 077

Nr.	Item	Explanation
	Management of IT security incidents	
1.	Last update of this record	8 May 2020
2.	Reference number	77
	Part 1 – Article 31 of Regulation (EU) 2018/1725 - Record (recommendation: Publicly available)	
3.	Name and contact details of the controller and of the staff member responsible	Controller: European Union Aviation Safety Agency (EASA) Staff member responsible: IT Security Manager Email: servicedesk@easa.europa.eu
4.	Name and contact details of DPO	dpo@easa.europa.eu
5.	Name and contact details of joint controller (where applicable)	n/a
6.	Name and contact details of processor (where applicable)	
7.	Purpose of the processing	Managing IT security incidents at EASA. This covers any event that leads potentially or actually to a damage to confidentiality, integrity or availability of information asset of EASA. In case of IT security incidents which may involve personal data, the DPO must be informed as soon as possible. Except in case of extreme urgency, accessing personal data of data subjects should only be carried out with the authorisation of the Head of IT. Except where a restriction listed in Article 25 of Regulation 2018/1725 applies, data subjects must be informed

		before the data is accessed or at the latest within one month after the data was accessed. This data may be processed for actions of investigation, containment, remediation and information relating to the incident.
8.	Description of categories of persons whose data are processed by EASA and list of personal data categories	Categories of persons whose data are processed by EASA: Individuals among the staff members and stakeholders involved in the incident e.g. Data Protection Officer, IT staff members and other EASA staff involved in the incident, individuals whose personal data may have been affected by the incident. Categories of personal data processed: - Identification data individuals among the staff members and stakeholders involved in the incident, - Personal information of individuals whose data may have been affected by the incident e.g. usernames, emails addresses, photos, cookies, IP related data, access and authorisation related data.
9.	Time limit for keeping the data	Personal data are kept for maximum 2 years after closure of the case. Personal data may be kept for longer if circumstances such investigations, appeals are ongoing at the planned expiration date.
10.	Recipients of the data	EASA IT staff members, EASA security officer, EASA Data Protection Officer, EASA Executive Director and other EASA staff on a need to know basis. Other recipients may be addressed on a case by case situation with the purpose of a good outcome of the incident such as the CERT-EU, the computer emergency response team of the EU institutions, bodies and Agencies or EASA processors.

11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No
12.	General description of security measures, where possible.	Operations are carried out in accordance with EASA internal IT security rules.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the below privacy statement.	See privacy statement

PRIVACY STATEMENT

[MANAGEMENT OF IT SECURITY INCIDENTS] [Ref # 077]

1. What personal data do we collect?

Categories of personal data processed:

- Identification data individuals among the staff members and stakeholders involved in the incident,

- Personal information of individuals whose data may have been affected by the incident e.g. usernames, emails addresses, photos, cookies, IP related data, access and authorisation related data.

2. For what purpose do we collect personal data and on which legal basis?

Managing IT security incidents at EASA. This covers any event that leads potentially or actually to a damage to confidentiality, integrity or availability of information asset of EASA.

The personal data is processed on the following basis:

Article 5(1)(a)of Regulation (EU) 2018/1725 read in conjunction with recital 22:

'Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body', which *'includes the processing of personal data necessary for the management and functioning of those institutions and bodies.'*

Article 75 of Regulation (EU) 2018/1139 on the establishment and functions of EASA.

3. Who may receive your personal data?

EASA IT staff members, EASA security officer, EASA Data Protection Officer, EASA Executive Director and other EASA staff on a need to know basis.

Other recipients may be addressed on a case by case situation with the purpose of a good outcome of the incident such as the CERT-EU, the computer emergency response team of the EU institutions, bodies and
Agencies or EASA processors.

4. How long are your personal data kept?

Personal data are kept for maximum 2 years after closure of the case. Personal data may be kept for longer if circumstances such investigations, appeals are ongoing at the planned expiration date.

5. What are your rights?

You have the right to request from EASA access to and rectification or erasure of your personal data or restriction of processing.

You also have the right to object to processing of your personal data.

EASA should provide information on action taken on a request within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

A breach concerning your personal data should be communicated to you under certain circumstances. EASA should also ensure the confidentiality of electronic communications.

6. Who is the data controller and how to exercise your rights?

EASA should exercise the tasks of the data controller for the purpose of these processing operations.

To exercise the mentioned rights, you can contact the controller by sending an email to: servicedesk@easa.europa.eu.
If you consider your data protection rights have been breached, you can always lodge a complaint with the EASA's Data Protection Officer (dpo@easa.europa.eu) or with the European Data Protection Supervisor: edps@edps.europa.eu.