European Union Aviation Safety Agency

FO Personal data processing records and compliance checklist - Public	Ref # 055

Nr.	Item	Explanation
	Access Control to EASA premises	
1.	Last update of this record	*13/01/2021*
2.	Reference number	*055*
	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) Postal address: Postfach 10 12 53, D-50452, Cologne, Germany Office address: Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany Telephone: +49 221 8999 000 Staff member responsible: Head of Relationship & Corporate Services Department E-mail: RS.3.3.Admin@easa.europa.eu
4.	Name and contact details of DPO	dpo@easa.europa.eu
5.	Name and contact details of joint controller (where applicable)	Not applicable
6.	Name and contact details of processor (where applicable)	Siemens AG Abteilung Smart Infrastructure Franz-Geuer-Str. 10 50823 Köln

7.	Purpose of the processing	The access control system aims at providing: • Security and safety measures to protect the persons and premises. • Authorisation of access to site and information about time spent on site. • Physical protection of the site. • Protection of organisational assets.
8.	Description of categories of persons whose data are processed by EASA and list of personal data categories	Categories of persons: EASA staff (including trainees, SNE's, interims, etc.), visitors, consultants, contractors and any person who requires to get access to the EASA building Categories of data: For **staff members, contractors and consultants** with permanent access badges, the data collected includes name and family name, type of contract, photo, personnel or identification number, period of access in the building. When a badge is swiped at the doors/elevators, the data collected includes a timestamp, ID of doors, badge number. Also, when issuing personalized permanent access badges for consultants and external service providers. In this case, Security office collects a declaration form "Certificate of good conduct". For **contractors and consultants** with loan badges, the form included in INSTR.RS.3.3.001 is filled with the following data: company name and address, period and nature of activity in the building, names and contact details of persons getting access and their superiors. Based on the form, loan badges are issued. When a badge is swiped at the doors/elevators, the data collected includes a timestamp, ID of doors, badge number. For **visitors** invited for a specific meeting (via "EASA roombooking tool"), the data collected includes family and first name, email address, as well as organisation or company name that visitor represents. Visitors shall present the official identity document at the reception to activate the QR code that grants them access to the EASA conference center premises. Activation and use of QR code at turnstiles records the data of entries/exits of the specific visitor. Outside office hours, additional physical register is kept with name, family name, arrival and departure times. Exceptionally, during COVID-19 pandemic:

		Together with activation of QR code at the reception or receipt of the loan badge, visitors and contractors submit a signed COVID-19 information form with their data (name, family name, contact details and signature). This form is stored at the reception and is to be used only for contact tracing purposes in case COVID-19 cases are identified after the visit to EASA.
9.	Time limit for keeping the data	Physical registers/paper forms are kept for 1 year after expiry of access authorization. Exceptionally, during COVID-19 pandemic: Visitor's and contractors' COVID-19 information related form is stored in accordance with *Corona Schutzverordnung.*
10.	Recipients of the data	EASA Security Health & Safety Officer, Corporate Services Section staff working with "roombooking tool", security guards, reception (EASA contractors), always on "a need to know" basis with different access level rights set in the system. Managers and investigators when requested in the framework of administrative enquiries or disciplinary procedures. Contract managers may also have access to this data to control time stamps data of external contractors. Data collected in COVID-19 information related form can be shared with health competent authorities and EASA Medical Service for contact tracing only in case COVID-19 cases are identified.
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.	The software for the computerised access control system is installed on only one computer on the Agency side, located in the office of the Security, Health & Safety Officer with controlled access from other staff members. The authentication criteria for the computerised system are known only to the Security, Health & Safety Officer on the side of the Agency, and Security Team leader on the side of the external security services provider. The physical register of presence outside office hours is kept in the security centre which is manned at all times by a guard. Data is safely disposed after the end of retention period. COVID-19 information related forms for tracing purposes are stored at EASA Reception which is manned at all times

		and are protected by keeping them locked. Data is safely disposed after the end of retention period.
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

Access Control to EASA premises Ref # 055

1. What personal data do we collect?

For staff members, contractors and consultants with permanent access badges, the data collected includes name and family name, type of contract, photo, personnel or identification number, period of access in the building. When a badge is swiped at the doors/elevators, the data collected includes a timestamp, ID of doors, badge number.

For contractors and consultants with loan badges, the form included in INSTR.RS.3.3.001 is filled with the following data: company name and address, period and nature of activity in the building, names and contact details of persons getting access and their superiors. Based on the form, loan badges are issued. When a badge is swiped at the doors/elevators, the data collected includes a timestamp, ID of doors, badge number.

For visitors invited for a specific meeting (via “EASA roombooking tool”), the data collected includes family and first name, email address, as well as organisation or company name that visitor represents. Visitors shall present the official identity document at the reception to activate the QR code that grants them access to the EASA conference center premises. Activation and use of QR code at turnstiles records the data of entries/exits of the specific visitor.

Outside office hours, additional physical register is kept with name, family name, arrival and departure times.

Exceptionally, during COVID-19 pandemic:
Together with activation of QR code at the reception or receipt of the loan badge, visitors and contractors submit a signed COVID-19 information form with their data (name, family name, contact details and signature). This form is stored at the reception and is to be used only for contact tracing purposes in case COVID-19 cases are identified after the visit to EASA.

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

The access control system aims at providing:

- Security and safety measures to protect the persons and premises.
- Authorisation of access to site and information about time spent on site.
- Physical protection of the site.
- Protection of organisational assets.

The legal basis for this processing operation can be found is Article 5(1)(a) of Regulation (EU) 2018/1725 in relation with Article 75 of Regulation (EU) 2018/1139.

3. Who may receive your personal data?

EASA Security Health & Safety Officer, Corporate Services Section staff working with “roombooking tool”, security guards, reception (EASA contractors), always on “a need to know” basis with different access level rights set in the system.
Managers and investigators when requested in the framework of administrative enquiries or disciplinary procedures.
Contract managers may also have access to this data to control time stamps data of external contractors.
Data collected in COVID-19 information related form can be shared with health competent authorities and EASA Medical Service for contact. tracing only in case COVID-19 cases are identified.

4. How long are your personal data kept?

Physical registers/paper forms are kept for 1 year after expiry of access authorization.

Exceptionally, during COVID-19 pandemic:
Visitor’s and contractors’ COVID-19 information related form is stored in accordance with *Corona Schutzverordnung.*

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 Head of Relationship & Corporate Services Department, e-mail RS.3.3.Admin@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.