



European Union Aviation Safety Agency

FO Personal data processing records and compliance checklist - Public	Ref Prevention & Mitigation of COVID 19 072
---	---

Nr.	Item	Explanation
Prevention & Mitigation of COVID 19 pandemic		
1.	Last update of this record	24.11.2021
2.	Reference number	072 v2
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: Security, Health & Safety Officer and Covid Team covid_med@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)	N/A
7.	Purpose of the processing	Personal data strictly necessary for the purpose of <ul style="list-style-type: none"> Allowing staff members access to EASA premises in accordance with the rules applicable to organisations established in Germany (notably the Infektionsschutzgesetz, as last amended 22.11.2021) and in the state of NRW: Name and Surname Staff number 1 of the 3 G evidence checked (vaccinated/recovered/test)





FO Personal data processing records and compliance checklist - Public	Ref Prevention & Mitigation of COVID 19 072
---	---

		<ul style="list-style-type: none">Identifying and supporting staff members infected or allegedly infected by the COVID 19 virus and mitigating the corresponding risks may be collected. This personal data may be emails from staff members describing their medical condition and notes from the EASA Medical advisors.
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: EASA staff members, visitors, contractors accessing or granted access to the EASA premises on a regular basis. Categories of personal data processed: staff member detail (as above), 3 G evidence, infection status (in case a COVID infection is confirmed).
9.	Time limit for keeping the data	Personal data collected to enable access to EASA's premises will be kept up to 19.03.2022 as per Art. 28b Infektionsschutzgesetz, or up to the time (earlier or later) required by the above mentioned law. Personal data collected to identify and support staff members infected or allegedly infected by the COVID 19 will be deleted as soon as the staff member provides proof of recovery or negative test.
10.	Recipients of the data	Reception employees designated to perform the checks EASA Medical Advisors Health and Security Officer
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.	Entry check lists will be held in the EASA systems, with restricted access.





European Union Aviation Safety Agency

FO Personal data processing records and compliance checklist - Public	Ref Prevention & Mitigation of COVID 19 072
---	---

		Data processed in the context of infection or status of vaccination will only be held by the EASA Medical Advisors observing strict professional secrecy.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the below privacy statement.	Please see Privacy Statement.





PRIVACY STATEMENT

PREVENTION AND MITIGATION OF COVID 19 PANDEMIC - Ref 072

1. What personal data do we collect and how do we collect it?

Personal data strictly necessary for the purpose of

- Allowing staff members access to EASA premises in accordance with the rules applicable to organisations established in Germany (notably the Infektionsschutzgesetz, as last amended 22.11.2021) and in the state of NRW:

Name and Surname

Staff number

1 of the 3 G evidence checked (vaccinated/recovered/test)

In case the evidence presented is the vaccination certificate, staff members may chose to present it at the reception (paper certificate or a digital certificate), or to send it to the medical service, covid_med@easa.europa.eu. The verification will be performed only once, through one of the following means:

- By the receptionist who will verify in the displayed information its validity, as well as if the name in the certificate corresponds to the name of the staff member as written in the ID document provided (e.g. EASA badge);
- By the medical doctor (covid-med) who will verify the validity of the certificate and its correspondence with identify of the certificate holder. Once the verification is done, the medical doctor will delete the certificate but will "tick off" your first and last names on the list.

The validity check may also be performed with the support of [CovPass Check App](#). This Application developed by Robert Koch Institute (**RKI**) is aimed to perform validity checks only, no data is processed or kept within the tester after the check is done. The data processed by this application is limited to the following:

QR codes scanned with CovPass and the information red from them are not permanently stored on the smartphone of the tester. In addition, the RKI does not store any personal data permanently on the server system of the app.

No registration: No registration with an e-mail address is necessary to show/use the CovPass.

No data storage: The data remains on the smartphone of the tested person.





FO Personal data processing records and compliance checklist - Public	Ref Prevention & Mitigation of COVID 19 072
---	---

Data economy: After checking the QR code, only the status of the certificate, the name and the date of birth are displayed on the screen.

When using CovPass and in order to download the public keys for the authentication of the electronic signature as well as the current rules for the validity of the certificates, a connection to a server of the RKI is regularly established. Technical access data is processed by the server. These include the following data: 1) IP address, 2) Date and time of retrieval, 3) amount of data transferred (or packet length), 4) Message whether the data exchange was successful. This access data is processed to enable and secure the connection and data exchange between the app and the server. You will not be personally identified as a user of the CovPassCheck app and no usage profile will be created. The IP address is not stored beyond the end of the individual usage process.

Cryptographic security: The QR code is secured with a signature that prevents counterfeiting.

Only EASA devices attributed to the recipients of data authorised to perform the checks are used, staff from the reception, medical doctor and the EASA Security, Health & Safety Officer.

- Identifying and supporting staff members infected or allegedly infected by the COVID 19 virus and mitigating the corresponding risks may be collected. This personal data may be emails from staff members describing their medical condition and notes from the EASA Medical Advisors.

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

The purpose of the processing of personal data is to comply with the employer's duty of care, by preventing COVID-19 contagion within the workplace, keeping EASA a safe place to work and ensuring continuity of business, securing and to protecting staff members' health from SARS-CoV-2 infection in compliance with the Staff Regulations and German National and Regional rules applied to employers in the context of COVID-19 prevention and mitigation measures.

Data may also be collected to identify and support staff members infected or allegedly infected by the COVID 19 virus and to mitigate the corresponding risks.

We process your personal data based on Article 5(1)(a) and (b) of Regulation (EU) 2018/1725 as the processing is necessary for the performance of a task carried out in the public interest and for compliance with a legal obligation to which the controller is subject. We carry out this operation based on:

- Article 1(e) of the EU Staff Regulations: 'Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant





FO Personal data processing records and compliance checklist - Public	Ref Prevention & Mitigation of COVID 19 072
---	---

to the Treaties.', applicable by analogy to by virtue of Article 10(1) and Article 80(4) of the Conditions of Employment of Other Servants of the EU (CEOS). Ref. Ares(2020)1562888 - 13/03/2020

- Processing of special categories of data is based on Article 10(2)(b) of Regulation (EU) 2018/1725
- Infektionsschutzgesetzes, as last amended 22.11.2021, und weiterer Gesetze anlässlich der Aufhebung der Feststellung der epidemischen Lage von nationaler Tragweite vom 22.11.2021.

3. Who may receive your personal data?

Your 3 G evidence will be processed by the receptionists upon your entrance in the building. According to the evidence shown, the receptionist will tick the respective box associated to your name and staff number. The data may also be received by the EASA Security, Health & Safety Officer.

If you have voluntarily provided EASA staff vaccination certificate to covid_med@easa.europa.eu, it will be verified by EASA Medical advisors. The receptionists from EASA Medical Advisors will receive only information that you comply with 3 G rules.

EASA Medical Advisors will receive the lists resulting from this entry check, which will be kept confidential. When requested, anonymized lists may be disclosed to national health authorities. Personal data collected to identify and support staff members infected or allegedly infected by the COVID 19 will be received by the EASA Medical Advisors.

4. How long are your personal data kept?

Personal data collected to enable access to EASA's premises will be kept up to 19.03.2022 as per Art. 28b Infektionsschutzgesetz, or up to the time (earlier or later) required by the above mentioned law.

Where the 3 G evidence chosen is the vaccination certificate, submitted to either the staff at the reception, or to the medical service, the check will be performed only once. Only the verification check will be kept, all other information contained in the certificate will be deleted as soon as the verification is performed. This also includes deletion of certificates provided to covid_med@easa.europa.eu via e-mail.

Personal data collected to identify and support staff members infected or allegedly infected by the COVID 19 will be deleted as soon as the staff member provides proof of recovery or negative test.





FO Personal data processing records and compliance checklist - Public	Ref Prevention & Mitigation of COVID 19 072
---	---

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.

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 covid_med@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

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

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.

