EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

DATA PROTECTION NOTICE

Digital verification of COVID-19 certificates upon entry of FRA premises

The European Union Agency for Fundamental Rights (FRA or Agency) processes the personal data of a natural person in compliance with Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

This data protection notice explains FRA's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognise that information privacy is an ongoing responsibility, and we will update this notice where necessary.

1. Why do we collect personal data?

The objective of this procedure is to prevent COVID-19 contagion and protect the health and safety of staff and non-staff in the FRA premises from a SARS-CoV-2 infection. While mandatory face masks, social distancing, body temperature screening and the reduced presence at the office already offer a good level of protection for staff and non-staff, it is appropriate to limit temporarily the access to the FRA premises, unless a valid COVID-19 certificate is presented.

Manual verification of COVID-19 certificates alone involves a significant risk of fraud, which poses a risk to FRA staff and non-satff members' health. It is necessary to ensure that the COVID-19 certificates have not been forged and that they belong to the persons presenting them. Verifying the validity and authenticity of the COVID-19 certificates can only be achieved effectively by using a scanning solution for validation of the QR codes displayed on COVID-19 certificates, while processing the minimum amount of personal data and without recording the results of the check, nor the content of the certificates.

The digital verification of COVID-19 certificates is a temporary measure and will be subject to a periodic review.

2. What kind of personal data does the Agency collect?

We will collect only the following personal data necessary for the processing operation described above.

(a) General personal data:

- Personal details (name, surname and date of birth)

(b) Special categories of personal data:

- Data concerning health: COVID-19 certificate [verifying the validity of the digital (exceptionally paper-based) certificate for vaccination against Covid-19, recovery from Covid-19 or for a negative PCR test. In exceptional cases, like in delay getting the PCR test, an antigen test can be accepted]

3. How do we collect your personal data?

The verification of certificates is carried out when entering the FRA premises in Vienna by the "Certificate Screening Operators" (CSOs) (e.g. the security guards) that have received appropriate training in the visual and automated method of screening COVID-19 certificates and the relevant workflow.

The digital verification of COVID-19 certificates is carried out by means of the mobile applications offered by the Austrian authorities ("Green check"). It is carried out by the "Certificate Screening Operators" (CSOs) (e.g. security guards). The certificates concerned are those mentioned in Director's Decision CS/0022/2021, as amended by decisions CS/0026/2021 and CS/008/2022.

The hand-held reader will be held in a way that discreetly shows the results on the screen only to the CSOs:

- Certificate is valid: the normal security entrance procedure applies and the person may enter;

- Certificate is not valid: the person is refused access for the day.

The CSOs also verify that the name and date of birth indicated on each certificate correspond to the information contained in the person's ID documents.

A manual verification of the certificates by means of a visual check may be carried out in case of technical problems with the digital verification by means of the mobile applications.

In case staff or non-staff members have non-valid certificates, they will not be allowed entry in the building, but they may request an 'Entrance Denied' certificate, which will not be personalized and only state that access to the building was denied on a certain date.

Your personal data will not be used for an automated decision-making including profiling.

4. Who is responsible for processing your personal data?

The Agency is the legal entity responsible for the processing of your personal data and determines the objective of this processing activity. The Head of Corporate Services is responsible for this processing operation.

Security guards employed by the security services provider contracted following a public procurement procedure (Securitas GmbH) will perform the digital verification verification of COVID-19 certificates upon entry of FRA premises.

5. Which is the legal basis for this processing operation?

The digital verification of COVID-19 certificates upon entry of FRA premises is necessary for the management and functioning of the Agency. Concretely, the legal basis is provided in the Director's Decision CS/008/2022 (Amendment No 2 to Director's decision CS/0022/2021 on Specific health and safety rules at FRA premises linked to SARS-CoV-2).

Therefore, the processing is lawful under Article 5.1.(a) of the Regulation (EU) No 2018/1725.

Moreover, this processing operation is necessary for compliance with a legal obligation of EU law to which the Agency is subject.

More specifically, the legal bases for this processing operation are:

- Staff Regulations of Officials of the European Union, and in particular Article 1e(2) thereof
- Conditions of Employment of Other Servants of the European Union (CEOS), and in particular Articles 10(1) and 80(4) thereof

Therefore, the processing is also lawful under Article 5.1.(b) of the Regulation (EU) No 2018/1725.

6. Who can see your data?

The FRA security guards under the supervision of the Digital Services and Facilities Sector have access to the personal data at hand for the purpose of the QR Code scanning and allowing access to the FRA premises.

7. Do we share your data with other organisations?

Personal data is processed by the Agency only. In case that we need to share your data with third parties, you will be notified to whom your personal data has been shared with.

8. Do we intend to transfer your personal data to Third Countries/International Organizations?

No.

9. When we will start the processing operation?

We will start the processing operation following the entry into force of Director's Decision CS/008/2022 (Amendment No 2 to Director's decision CS/0022/2021 on Specific health and safety rules at FRA premises linked to SARS-CoV-2).

10. How long do we keep your data?

No personal data is retained by FRA. Data is not stored, the information only appears on the screen of the mobile phone and is deleted from the mobile device cache-memory immediately after indicating the certificate validity status with Green (valid) or Red (not valid). There is no storage of personal data on a permanent memory.

11. How can you control your data?

Under Regulation 2018/1725, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information. You are not required to pay any charges for exercising your rights except in cases were the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

We will reply to your request without undue delay and in any event 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.

You can exercise your rights described below by sending an email request to facilities@fra.europa.eu

11.1. The value of your consent

Since the processing operation will lawfully take place under Article 5.1.(a) (processing is necessary for the management and functioning of the Agency), and 5.1.(b) of Regulation (EU) No 2018/1725 (processing is necessary for compliance with a legal obligation to which the controller is subject) -see Section 5 of this Data Protection Notice above- you are not required to provide your consent.

Should you object to the digital verification of your COVID-19 certificate, you will not be permitted to enter the FRA premises.

11.2. Your data protection rights

a. Can you access your data?

You have the right to receive information on whether we process your personal data or not, the purposes of the processing, the categories of personal data concerned, any recipients to whom the personal data have been disclosed and their storage period. Furthermore, you can have access to such data, as well as obtain copies of your data undergoing processing.

b. Can you modify your data?

You have the right to ask us to rectify your data you think is inaccurate or incomplete at any time.

c. Can you restrict us from processing your data?

You have the right to restrict the processing of your personal data. If you do, we can no longer process them, but we can still store them. In some exceptional cases, we will still be able to use them (e.g. with your consent or for legal claims). You have this right in a few different situations: when you contest the accuracy of your personal data, when the Agency no longer needs the data for completing its tasks, when the processing activity is unlawful, and finally, when you have exercised your right to object.

d. Can you delete your data?

Under Regulation 2018/1725, you have the right to ask us to delete your data when the personal data are no longer necessary for the purposes for which they were collected, when you have withdrawn your consent or when the processing activity is unlawful. In certain occasions we will have to erase your data in order to comply with a legal obligation to which we are subject.

We will notify to each recipient to whom your personal data have been disclosed of any rectification or erasure of personal data or restriction of processing carried out in accordance with the above rights unless this proves impossible or involves disproportionate effort from our side.

Please note that, within this particular processing operation, no (personal) data is stored by FRA.

e. Are you entitled to data portability?

Data portability is a right guaranteed under Regulation 1725/2018 and consists in the right to have your personal data transmitted to you or directly to another controller of your choice.
In this case, this does not apply for two reasons: I) in order for this right to be guaranteed, the processing should be based on automated means, however we do not base our processing on any automated means; II) this processing operation is carried out in the public interest, which is an exception to the right to data portability in the Regulation.

f. Do you have the right to object?

When the legal basis of the 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 is the case in most of our processing operations, you have the right to object to the processing. In case you object, we have to stop the processing of your personal data, unless we demonstrate a compelling reason that can override your objection.

g. Do we do automated decision making, including profiling?

Your personal data will not be used for an automated decision-making including profiling.

12. What security measures are taken to safeguard your personal data?

The Agency has several security controls in place to protect your personal data from unauthorised access, use or disclosure.

In particular, no personal data is stored in the context of the digital verification of COVID-19 certificates upon entry of FRA premises.

Moreover, access to the data is restricted to duly authorised personnel working in the premises of FRA in Vienna, who have been designated to carry out the verification process on the basis of the role (security guards) they perform within the Agency and are bound by the duty of confidentiality. These persons have also received appropriate training in the method of screening COVID-19 certificates.

The QR code scanning solely results in a confirmation of the authenticity, validity and integrity of the COVID-19 certificate in question, also in accordance with the data minimisation principle. In addition, the security guards will place the screen of their devices in a way that does not allow any other person to see the result of the scanning of the certificates.

13. What can you do in the event of a problem?

a) The first step is to notify the Agency by sending an email to facilities@fra.europa.eu and ask us to take action.

b) The second step, if you obtain no reply from us or if you are not satisfied with it, contact our Data Protection Officer (DPO) at dpo@fra.europa.eu.

c) At any time you can lodge a complaint with the EDPS at http://www.edps.europa.eu, who will examine your request and adopt the necessary measures.

14. How do we update our data protection notice?

We keep our data protection notice under regular review to make sure it is up to date and accurate.

END OF DOCUMENT