EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: Digital verification of COVID-19 certificates upon entry of FRA premises

Reference number: DPR-2022-144
Creation date of this record: 18/01/2022
Last update of this record:
Version: 1

Part 1 (Publicly available)

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA)
Schwarzenbergplatz 11, A-1040 Vienna, Austria
Telephone: +43 1 580 30 – 0
Email: contact@fra.europa.eu
Organisational unit **responsible**[4] for the processing activity: Corporate Services
Contact details: *facilities@fra.europa.eu*
Data Protection Officer (DPO): dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by a third party (contractor) [mention the third party]	☒

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

2 **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.
Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

4 This is the unit that decides that the processing takes place and why.

5 Is the FRA itself conducting the processing? Or has a provider been contracted?

(Security guards employed by the security services provider contracted following a public procurement procedure (Securitas GmbH).

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).

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, 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-staff 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 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.

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

4) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

FRA staff (including SNEs and trainees) ☒

Non-FRA staff (e.g. every person contractually involved with FRA, visitors, and all other individuals entering the FRA premises) ☒

5) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate

(a) **General personal data (add or delete as appropriate – the data in the brackets are only examples)**

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

Contact details (e.g. postal address, email address, mobile and fax number) ☐

Education & Training details ☐

Employment details (e.g. work experience, languages, name and type of the employer/organisation, address of the employer/ organisation) ☐

Financial details (e.g. financial identification form, bank account information) ☐

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details):

(b) **Special categories of personal data** (Article 10)
The personal data collected reveal:

Racial or ethnic origin ☐

Political opinions ☐

Religious or philosophical beliefs ☐

Trade union membership ☐

Genetic, biometric or data concerning health ☒

-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.]
☒

Information regarding an individual's sex life or sexual orientation ☐

N/A ☐

(c) **Personal data relating to criminal convictions and offences** (Article 11)

Criminal record (or similar, e.g. declaration of good conduct) ☐

N/A ☐

6) Recipient(s) of the data (Article 31.1 (d))

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).*

Designated **FRA** staff members
(please specify which team and Unit-no need to mention specifically the names of colleagues) ☒

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.

Recipients **outside** FRA:
(please provide a generic/functional mailbox) ☐

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

7) Transfers to third countries or international organisations (Article 31.1 (e))[6]

If the personal data are transferred outside the European Economic Area or to international organisations, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Transfer outside of the EU or EEA

Yes ☐

No ☒

If yes, specify to which country:

Transfer to international organisation(s)

Yes ☐

No ☐

If yes specify to which organisation:

Legal base for the data transfer

☐ Transfer on the basis of the European Commission's adequacy decision (Article 47)

☐ Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

a) ☐ A legally binding and enforceable instrument between public authorities or bodies.

Standard data protection clauses, adopted by

b) ☐ the Commission, or

c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .

d) ☐Binding corporate rules, ☐ Codes of conduct , ☐ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:
☐ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an international agreement (Article 49), specify:

Derogations for specific situations (Article 50.1 (a) –(g))

☐ N /A

[6] **Processor** in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply
In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

☐ (a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
☐ (b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
☐ (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
☐ (d) The transfer is necessary for important reasons of public interest
☐ (e) The transfer is necessary for the establishment, exercise or defense of legal claims
☐ (f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
☐ (g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g. in selection procedures candidates who made it onto the reserve list vs. those who didn`t). Are the data limited according to the adage "as long as necessary, as short as possible"?

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.

9) Technical and organisational security measures (Article 31.1(g))

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor

How is the data stored?

Document Management System (DMS) ☐

FRA network shared drive	☐
Outlook Folder(s)	☐
CRM	☐
Hardcopy file	☐
Cloud (give details, e.g. cloud provider)	☐
Servers of external provider	☐
N/A	☒

-No personal data is stored nor memorised in the devices used for the QR code scanning and the information is not sent or transmitted anywhere.

10) Exercising the rights of the data subject (Article 14 (2))

How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?

See further details in the Data Protection notice: e-mail to facilities@fra.europa.eu

Data subject rights

- ☒ Right of access
- ☒ Right to rectification
- ☐ Right to erasure (right to be forgotten)
- ☒ Right to restriction of processing
- ☐ Right to data portability
- ☒ Right to object
- ☒ Notification obligation regarding rectification or erasure of personal data or restriction of processing
- ☒ Right to have recourse
- ☐ Right to withdraw consent at any time