EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION ON THE EUROPEAN COMISSION'S DRAFT INTERNAL RULES ON DIGITAL VERIFICATION OF COVID-19 CERTIFICATES

INTRODUCTION

- This Opinion relates to the European Commission's (the Commission) request for a formal consultation on its draft internal rules on digital verification of COVID-19 certificates, submitted to the EDPS on 14 October 2021.
- The EDPS issues this Opinion in accordance with Article 58(3)(c) of Regulation (EU) 2018/1725[1], ('the Regulation').
- The EDPS regrets that he has been consulted at this stage of the procedure. His assessment in the present opinion is the outcome of the limited time available to issue his opinion, following receipt of the request.

BACKGROUND INFORMATION

By letter of 14 October 2021, the Commission consulted the EDPS on its draft internal rules ('draft Decision') on digital verification of COVID-19 certificates for visitors in the Commission's buildings in Brussels and Luxemburg. For the purpose of the consultation, the Commission communicated to the EDPS the draft Commission Decision amending Decision C(2020) 5973 as regards the digital verification of COVID-19 certificates and its Protocol on digital scanning of COVID-19 certificates. The EDPS acknowledged receipt of the consultation request on the same day.

According to the information received, the Commission intends to deploy the use of hand-held mobile devices containing a QR code-reading app, in order to check visitors' vaccination, test or recovery certificates ('COVID-19 certificates' or 'certificates') before granting them access to the Commission's buildings in Brussels and Luxemburg. The

[1] Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 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, OJ, L 295, 21.11.2018, pp. 39-98.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

screening of the COVID-19 certificates will be carried out by non-medical staff (e.g. guards), the Certificate Screening Operators ('CSOs'), who have received appropriate training in the visual and automated method of screening COVID-19 certificates and the relevant workflow. The CSOs will use specific mobile apps identified in the draft Decision. They will place the screen of their devices in a way that does not allow any people other than themselves to see the result of the scanning of the certificates on it. The result of the screening will be either valid, when a green check mark appears on the screen, or invalid, when a red exclamation mark appears. In cases where the screening of the QR code of the certificates is not possible, for example when there are technical problems, or upon request of the visitor, checks of the certificates will be carried out manually by the CSOs.[2]

Screening of the certificates will take place inside the building, but before or at the level of the security check gates (transit zone). Clear indications that the certificate check will take place, as well as the relevant data protection information (e.g. privacy notice and reference to the appropriate data protection record) must be visible upon entering the screening zone.

The name of the visitors, the content of the certificate and the result of the digital verification shall not be stored, transferred or otherwise processed. In case a visitor is in the possession of a non-valid certificate, they will not be allowed entry in the building that day. The name of visitor or any other personal data or data relating to health shall not be recorded, stored or transferred to any other service. Upon request of a visitor who has been denied entry in the building, an 'Entranced Denied' certificate can be issued. Such certificate will not be personalised and will only state that access to the building was denied on a certain date.

LEGAL ANALYSIS AND RECOMMENDATIONS

Lawfulness of the processing

The processing operation as described above, i.e. digital verification of certificates involving the scanning of a QR code, constitutes processing as defined by Article 2(5) of the Regulation and, therefore, falls within the scope of the Regulation. The EDPS considers that the processing in question interferes with the individuals' fundamental rights of privacy and data protection.

The Commission bases such processing on Article 5(1)(a) of the Regulation, it being reportedly necessary for the performance of a task carried out in the public interest. Pursuant to Article 5(2) of the Regulation, the basis for such processing shall be laid in Union law, which the draft Decision provides. The processing in question may reveal personal data concerning health, such as data relating to the vaccination status, test results or recovery from a COVID-19 infection. Health data is considered a special category of personal data, the processing of which is in principle prohibited under Article 10(1) of the Regulation. The processing of such data for the purpose of digital verification of COVID-19 certificates on the basis of the draft Decision falls under the exceptions of Articles 10(2)(b), (g) and (i) of the Regulation. Furthermore, processing is also based on Article 1e(2) of the Staff Regulations, since the Commission acts as the data controller in the field of employment and social security and is obliged to draw measures intended to protect the health and safety of its

[2] Manual verification of COVID-19 certificates falls outside the scope of the Regulation and will therefore not be analysed within the present opinion.

staff members. This legal basis can equally apply to processing of personal data of non-staff members by the Commission.

Reference to the aforementioned legal bases is made in the recitals of the draft Decision.

Recommendation 1: While the EDPS considers the processing in question lawful, he recommends that the Commission make reference to the legal bases in the body of the draft Decision, the operative part of the text, and not solely in the recitals.

Necessity and proportionality of the processing, and appropriate safeguards

Article 52 (1) of the Charter of Fundamental Rights of the European Union ('the Charter') provides that, subject to the principle of proportionality, limitations on the exercise of the fundamental rights and freedoms recognised by the Charter may be made only if they are necessary.

A limitation may be necessary if there is a need to adopt measures for the public interest objective pursued. Necessity also implies that the measures adopted must be less intrusive compared to other options for achieving the same goal. In case a measure is found to be necessary, then its proportionality needs to be assessed too. Proportionality means that the advantages resulting from the limitation should outweigh the disadvantages the latter causes on the exercise of the fundamental rights at stake. To reduce disadvantages and risks to the enjoyment of the rights to privacy and data protection, it is important that limitations contain appropriate safeguards.

The Commission's aim with the deployment of the processing in question is to protect the health and safety of its staff in Brussels and Luxemburg, by preventing the further spread of COVID-19, while ensuring at the same time business continuity. Re-purposing certificates for the use envisaged by the Commission, i.e. visitors' entry into its buildings, should clearly aim to reduce the risk of transmission and protect employees from infection. To assess the necessity of the proposed measure, the Commission should take into account parameters such as infection prevalence in the general population, transmission dynamics in its buildings and exposure risk of staff.

In addition to its assessment in Commission Decision C(2021) 6669, the Commission points out that there are progressively more cases of illicit high-quality counterfeit COVID-19 certificates. Ensuring that presented certificates are not forged and belong to the persons presenting them could only be achieved effectively by using a scanning solution for validation of the QR codes displayed on certificates. The Commission highlights that less intrusive alternatives have been explored, but rejected; the collection of aggregated data regarding vaccination status of visitors prior to their arrival would not allow to identify specific individuals that should not be granted access to the sites due to the health risk that they might pose. Furthermore, digital screening of certificates is more reliable and efficient than manual screening.

The EDPS takes note of the fact that the draft Decision makes no reference to other less intrusive controls, such as organisational arrangements to ensure physical distancing and sanitary precautions.

In line with the principle of data minimisation, the draft Decision provides for processing limited to what is necessary for the initial verification, and does not include recording,

storage, transmission or otherwise processing of personal data. Indeed, most QR code verification applications display only a subset of the data encoded in the QR. However, since the Commission intends to employ the mobile apps CovidScan and CovidCheck.lu to verify certificates issued in accordance with Article 3(1) of Regulation (EU) 2021/953 as stipulated in Recital 5 and 13 of the draft Decision, more personal data are processed than what is currently listed under Article 2c(2).

It follows from the certificate specification[3] that a unique certificate identifier, the country of vaccine application, the certificate issuer and the number in a series of doses are among the information processed with every scan of a QR code. These meta-data allow inference, for instance, of the place of residence during the pandemic or of information relating to whether a visitor has received early on a booster shot or belongs to a priority group within the vaccination campaign. Consequently, vulnerable people might be identified as such. In addition, the precise indication of the vaccine constitutes unnecessarily additional information, whereas an indication that the used vaccine fulfils the requirements laid down in Regulation 2021/953 would have been sufficient.

Therefore, the EDPS notes that the present use case of QR codes is not entirely in line with the principles of data protection by design and by default and data minimisation.

In line with the principle of purpose limitation, the draft Decision provides for processing only for the purpose of being allowed entry in one of the Commission's buildings.

In line with the principle of transparency, information about the processing should be given to the individual before the processing starts, and it should also be readily accessible to them during the processing. The draft Decision provides that information about the processing 'shall be conveyed to the data subjects by means of privacy statements published on the website of the Commission, or by other means'.

The EDPS takes note of the fact that the envisaged processing provides for meaningful human involvement in the verification process and decisions on the entry or not into buildings are not based solely on automated processing.

The EDPS notes that Art 2c (4) of the draft Decision provides for the manual verification of corona certificates in the case the verification by means of the QR code fails or following the data subject's request. The EDPS stresses that the scanning of QR codes for the purpose of detecting forged certificates laid down in Recital 7 is only efficient if malicious actors cannot provoke the loosening of security standards by presenting a deliberately corrupted QR code.

As stipulated in Recital (13) of the draft Decision, the Commission provides for the use of national QR code verification applications. These applications process personal data including special categories of data. We note that there is no account that the Commission has assessed ex-ante whether these applications can lawfully process personal data, based on the principle of data protection by design and by default. The EDPS notes that the processing may fall within the scope of the EDPS Guidelines on the protection of personal data processed by mobile applications provided by European Union Institutions[4]. In any case, the EDPS invites the European Commission to consider carefully the attribution of controller and processor roles with respect to the processing by the mobile application and by the mobile operating system.

---

3 https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_json_specification_en.pdf

4 https://edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_mobile_apps_en.pdf

Finally, the EDPS notes that the envisaged processing is of an exceptional, temporary nature and shall apply until 31 March 2022, in line with the sunset clause included in Commission Decision C(2021) 6669.

Recommendation 2: The Commission needs to assess alternative measures relating to organisational arrangements that would ensure physical distancing and sanitary precautions and document the outcome of such assessment.

Recommendation 3: The Commission needs to provide for a verification procedure that does not allow malicious actors to bypass a verification of the digital certificate. Otherwise, its processing would be inefficient to achieve the goal to stop the use of forged certificates.

Recommendation 4: In order to facilitate data subjects' right to information regarding the processing of their personal data, the Commission needs to include data protection notices in the transit zone, where visitors will be having their certificates checked, for e.g. by means of posters on the walls or any other surface, visible to them. This will allow visitors to know in advance how verification will take place, what data will be processed, who will have access to it, and where to direct any queries or objections regarding the processing.

Recommendation 5: With respect to the data processing of verification apps, the Commission needs to assess the compliance of the apps used with the Regulation, based on the obligation of data protection by design and by default, and document such assessment.

Recommendation 6: The Commission needs to include in the draft Decision reference to the fact that the sunset clause shall be subject to periodic review and determine such review period.

CONCLUSION

In light of the accountability principle, the EDPS expects the Commission to implement the aforementioned recommendations accordingly, and has decided to **close the case.**

Done at Brussels on 18 October 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI