EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation on a framework for the issuance, verification and acceptance of the Digital Green Certificate

On 17 March 2021, the Commission published the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate).

The proposal aims at facilitating the exercise of the right to free movement within the EU during the COVID-19 pandemic by establishing a common framework for the issuance, verification and acceptance of interoperable certificates on COVID-19 vaccination, testing and recovery (Digital Green Certificate). It requires all member states to use the Digital Green Certificate and issue certificates to facilitate the right to free movement within the EU during the COVID-19 pandemic.

On 31 March 2021, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) issued a joint opinion (EDPB-EDPS Joint Opinion 04/2021) to evaluate whether the proposal is consistent and does not conflict with the fundamental right to the protection of personal data, as enshrined in art. 16 TFEU, art. 8 CFR and the GDPR.

This document summarises the main points of the EDPB-EDPS Joint Opinion 04/2021.

PRELIMINARY CONSIDERATIONS

Data protection is not an obstacle for fighting the pandemic. On the contrary, compliance with data protection law will help citizens' trust. Any proposal on this should take a holistic and ethical approach, and the principles of effectiveness, necessity and proportionality must guide any measure involving the processing of personal data.

The certificate should be understood as a verifiable proof of a timestamped factual medical application or history that will facilitate the free movement of EU citizens within the EU due to its common format in all member states, and not an immunity certificate.

The EDPB and the EDPS underscore that an impact assessment concerning the effectiveness of existing less intrusive alternatives is missing. Additionally, the risk of discrimination, the lack of a common approach towards interoperable certificates and the risk of forgery and sale of false test certificates still exist.

THE NEED FOR A COMPREHENSIVE LEGAL FRAMEWORK

According to art. 52 CFR, limitations to fundamental rights can only be made subject to the principle of proportionality and necessity. Hence the proposal should achieve a fair balance between the objectives pursued by the Digital Green Certificate and the individual interest in self-determination, and the fundamental rights to privacy, data protection and non-discrimination.

In the proposal proportionality is addressed when data processing is limited to the minimum necessary (art. 5 and Annex), by setting that data obtained when verifying certificates should not be retrained (art. 9), by not requiring a central database and by establishing that the framework is temporary.

The EDPB-EDPS consider that any possible other use of the framework and the Digital Green Certificate by national law, other than facilitating the free movement between member states, may lead to unintended consequences and risks to fundamental rights. Any such further use should not legally or factually lead to discrimination based on having been (or not) vaccinated or recovered from Covid-19. Therefore, any possible further use of the framework, the Digital Green Certificate and the personal data related to it at national level must respect arts. 7 and 8 CFR and GDPR, particularly art. 6(4) GDPR.

This implies:

- the need of a proper legal basis to process;
- complying with the principles of effectiveness, necessity, and proportionality;
- including safeguards following a DPIA, in particular to avoid discrimination;
- the prohibition of retention of data in the context of the verification process;
- the specification of the scope and extent of processing, and the categories of entities that can verify the certificate.

In this context, the EDPB-EDPS consider that:

- the proposal could better define the purpose of the Digital Green Certificate and provide for a mechanism for the monitoring of the use of the certificate; and

- provide that access and subsequent use of the data by member states once the pandemic has ended is not allowed.

SPECIFIC DATA PROTECTION-RELATED COMMENTS

Concerning the proposal, the EDPB-EDPS both supported and make suggestions.

To begin with, the EDPB-EDPS **welcomed** that the proposal:

- does not allow for the creation of any sort of personal data central database at EU level;
- requires that the certificates only contain the personal data necessary to attain the purpose of facilitating the exercise of the right to free movement within the EU during the pandemic;
- allows citizens to obtain and renew the certificates free of charge if their personal data is not or no longer accurate or up-to-date;
- clarifies the roles of controller and processor in the context of the certificate framework;
- does not create a legal basis for retaining personal data obtained from the certificate to implement certain public health measures during Covid pandemic and that data processed cannot be retained longer than is necessary.

On the other hand, the EDPB-EDPS **recommended** that the proposal should:

- clarify whether the certificate will be automatically created but only provided upon request of the data subject, or whether this will only be issued upon request of the data subject;
- make available certificates both in digital and paper-based formats, to ensure inclusion of all citizens;
- employ verification techniques that do not require transmission of personal data to third countries whenever possible;
- clarify the definition of 'interoperability' contained in art. 2(6);
- justify the need to include certain categories and data fields of personal data to be processed in Annex I;
- clarify whether all the categories of personal data provided for in Annex I need to be also included in the Quick Response (QR) code of both digital and paper-based certificates;
- specify the expiry date of the validity of each certificate (except for the certificate of recovery);
- provide additional substantiation, concerning the vaccination certificate, as to the need for data fields such as the vaccine medicinal product, vaccine marketing

authorisation holder or manufacturer and number in a series of vaccinations/doses to be included in the certificate;

- limit the Commission's power to add data fields on the categories of personal data of the three types of certificates via delegated acts to the inclusion of more detailed data fields (sub-categories of data) failing under the already defined categories of data;
- state that the controllers and processors must take technical and organisational measures to ensure a level of security appropriate to the risks of processing (art. 32 GDPR), e.g. processes for regular testing, and that further specification could be made by means of implementing acts by the Commission;
- specify that a list of all entities foreseen to be acting as a controller, processor and recipient of the data in that Member State must be made public;
- ensure that transparency of the processes are clearly outlined for the citizens to be able to exercise their data protection rights;
- define, where possible, specific data storage periods or at least specific criteria used to determine them, and that storage should not go beyond the end of the Covid pandemic;
- clarify explicitly whether and when any international transfer of personal data are expected and include safeguards in the legislation to ensure that third countries will only process personal data exchanged for the purposes specified by the proposal.

This briefing was prepared by Federico Marengo for QUBIT PRIVACY

QUBIT PRIVACY is a consultancy firm established in Italy that provides tailor-made services for individuals and companies to comply with the requirements established in the General Data Protection Regulation.

Qubit Privacy

Find more

https://qubitprivacy.com/

Federico Marengo is a lawyer, master in public administration (University of Buenos Aires), LLM (University of Manchester), and PhD candidate (Università Bocconi, Milano).
He currently provides data protection consultancy services for Qubit Privacy and also works as of counsel at Data Business Services.
He is the author of "Data Protection Law in Charts. A Visual Guide to the General Data Protection Regulation", e-book released in 2021, and authored several publications on international data transfers and international trade law.
As a PhD researcher, his research deals with the potential and challenges of the General Data Protection Regulation to protect data subjects against the adverse effects of Artificial Intelligence.
He is also teaching assistant at Università Bocconi.