As access to COVID-19 vaccines becomes more prevalent, and we begin to conceptualize what a post-pandemic world might look like, many governments are assessing the idea of a COVID-19 vaccine passport framework. In late March, the European Commission announced its plan for a COVID-19 Digital Green Certificate framework ("the framework") to facilitate "safe free movement of citizens within the EU during the COVID-19 pandemic". The Digital Green Certificate provides proof that an individual has either: 1) been vaccinated against COVID-19, 2) received a negative test result or 3) recovered from COVID-19. But while the benefits to such a plan are clear, there are significant privacy and security issues to consider.

Shortly after the European Commission released the proposal of the framework, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) issued a joint opinion on the framework in respect to personal data protection implications ("the joint opinion"). The joint opinion addressed the personal data implications of the framework, and highlighted, above all, that such a...
framework must be consistent and not conflict with application of the General Data Protection Regulations ("GDPR"), and that there should be adoption of adequate technical and organizational privacy and security measures in the context of the framework.

**Below are key recommendations from the joint opinion:**

- **Categories of Personal Data.** While Annex I of the framework sets out categories and data fields of personal data that would be processed under the framework, the joint opinion emphasizes that the “justification for the need for such data fields” should also be included in the framework, as well as developing “more detailed data fields (sub-categories of data)...under the already defined categories of data should be added”. These revisions will help ensure that the framework is consistent with several GDPR principles including data minimization (i.e. not processing more than the data necessary to fulfil the purpose for which the data was collected), purpose limitations (personal data shall only be collected for a specified, explicit and legitimate purpose), and impact assessment (the obligation under the GDPR which requires controllers to conduct a data protection impact assessment before processing personal data would have to be redone if data fields were altered).

- **Adoption of Adequate Technical and Organizational Privacy and Security Measures in the Context of the Proposal.** The joint opinion highlights that the framework should explicitly state that controllers and processors of personal data “shall take adequate technical and organizational measures to ensure a level of security appropriate to the risk of processing, in line with Article 32 GDPR”. Also included, the joint opinion suggests “the establishment of processes for a regular testing, assessment and evaluation of the effectiveness of the privacy and security measures adopted”, as well as including language in the framework consistent with the GDPR to prevent confusion and ensure relevance. Finally, the joint opinion notes that adoption of privacy and security measures should be taken both at the time of the determination of the means for processing, as well as by the time of the processing itself.

- **Identification of controllers and processors.** The joint opinion recommends that the framework specify “the list of all entities foreseen to be acting as controllers, processors and recipients of the data in that Member State”. Identifying these entities will provide EU citizens with an understanding of “whom they may turn to for the exercise of their data protection rights under the GDPR, including in particular the right to receive transparent information on the ways in which data subject’s rights may be exercised with respect to the processing of personal data”.

- **Transparency and data subject’s rights.** The personal data related to the framework is particularly sensitive. As a result, the joint opinion urges the European Commission to “ensure that the transparency of the processes are clearly outlined for citizens to able to exercise their data protection rights”.

- **Data storage.** The joint opinion notes that to ensure GDPR principles surrounding data storage principles (e.g. storing data no longer than is necessary for the purposes for which it was processed) in the context of the
framework, where possible, the framework should “explicitly define” and if not possible, then at least provide the “specific criteria used to determine such storage period”.

• **International data transfers.** Finally, the joint opinion recommends “explicitly clarifying whether and when any international transfers of data are expected” as well as including safeguards “to ensure that third countries will only process the personal data exchanged for the purposes specified” within the framework.

The EU is not the only region implementing or considering a vaccine passport program. Israel’s vaccine passport, the [Green Pass](https://greenpass.gov.il), is already up and running (available to the 80% of the adult population that is fully vaccinated), and several private companies are trying to develop globalized vaccine passport programs. For example, one large tech company’s vaccine passport technology is being tested by the State of New York, for some sports venues and arenas. Likewise, another technology, the [Common Pass](https://www.commonpass.com) if implemented will help individuals when travelling globally to demonstrate their COVID-19 status. It is worth noting however, that some states are actively banning vaccine passport technology and requirements. For example, just last week in Florida, Governor Ron DeSantis signed into law [legislation](https://www.legislature.state.fl.us/Session/2021/FirstSession/Laws/Chapters/19/19.010.htm) prohibiting businesses, schools and government offices from requiring proof of vaccination, with fines of up to $5000. And in general, public support of vaccine passports in the U.S. seems to vary by activity. According to a recent [Gallup poll](https://www.gallup.com/poll/370363/states-decision-on-vaccination-passports.aspx) the majority of Americans support proof of vaccination for travel by airplanes and attending events with large crowds. Conversely, Americans are less supportive of proof of vaccination at work, staying in a hotel or dining at a restaurant.

Whatever the program, the privacy and security considerations surrounding the collection of personal data are similar, and become increasingly complicated in the context of a global vaccine program where overlapping, and sometimes conflicting, data privacy and security laws and guidance come into play. In the U.S. alone, there are numerous laws which may be implicated when vaccine related data is collected from individuals in the public or private setting – such as for employees or customers. These include the Americans with Disabilities Act (ADA), the Genetic Information Nondiscrimination Act (GINA), state laws, and the CCPA. In addition to statutory or regulatory mandates, organizations will also need to consider existing contracts or services agreements which may provide for or limit the collection, sharing, storage, or return of data. Moreover, if a vendor were involved in a vaccine passport program, contracts/agreements would need to include confidentiality, data security, and similar provisions. This is most important if the vendor will be maintaining, storing, accessing, or utilizing the information collected about the organization’s employees or customers.

In short, a vaccine passport program may play a crucial role in ensuring a safe and healthy return to normalcy across the globe. Nevertheless, the legal risks, challenges, and requirements of any such program, whether in the public and private forum, must be considered prior to implementation.

Jackson Lewis P.C. © 2021