GPA COVID-19 Working Group: Compendium of Best Practices in Response to COVID-19 (Part II)

October 2021

Table of Contents

Executive Summary

Background

1. Since the end of December 2019, the world has been plagued with the COVID-19 pandemic. Nearly two years into the pandemic, governments around the world have taken many administrative and technological measures to contain the spread of the disease while striking a balance between public health and the need of resuming normal activities. Innovative solutions such as digital contact tracing and tracking, as well as digital proof of health and immunity for cross-border/boundary travel and domestic activities were created to address public health concern, yet they may have posed risk to individuals' privacy and data protection. The digital solutions therefore came into the purview of data protection authorities ("DPAs"). It is beyond doubt that the data protection measures and regulatory responses have been adopted in tandem with the unprecedented changes. 'New normal' is the term that has been adopted by governments, business owners and the public alike.

2. Against this background, the 42nd Global Privacy Assembly ("GPA") Closed Session held in October 2020 adopted the 'Resolution on the Privacy and Data Protection Challenges Arising in the Context of the COVID-19 Pandemic', which, among others, resolved to officially establish the COVID-19 Working Group ("Working Group"). The Working Group consists of two sub-groups, one focuses on exploring the best practices for emerging privacy issues during the COVID-19 pandemic, the other one focuses on capacity building for GPA members.

3. The GPA first established the COVID-19 Taskforce in May 2020, which was the predecessor of the COVID-19 Working Group. At the 42nd GPA Close Session, the COVID-19 Taskforce presented Part I of the 'Compendium of Best Practices in Response to COVID-19', which contained relevant experience and good practice contributed by 32 GPA members and observers in relation to several privacy issues arising from the COVID-19 pandemic.

4. Building on the work done by the COVID-19 Taskforce, the sub-group on emerging issues of the Working Group set a work plan in early 2021 to explore the relevant privacy and data protection issues arising from the pandemic in 2021. A first survey was conducted among GPA members and observers by the Working Group in March 2021, with the goal of finding out the most pressing privacy and data protection issues at that stage of the COVID-19 pandemic, as well as to determine the best way that the GPA and/or the Working Group may provide support to GPA members and the community on the issues concerned. The

following six privacy and data protection issues were identified to be the most pressing by the survey:

(1) Processing and sharing of personal data collected in vaccination programmes to facilitate cross-border/boundary travel and domestic activities;
(2) Processing and sharing of health data (e.g. COVID-19 test results), travel history and/or contact history to facilitate cross-border/boundary travel and domestic activities;
(3) Handling of health data in 'health passports' and / or 'health codes';
(4) Health monitoring of incoming travellers;
(5) Handling of personal data in contact tracing measures (e.g. contact tracing apps); and
(6) Handling of children's or students' data associated with the use of e-learning and online schooling technologies.

5. Based on the results of the aforesaid survey, a second survey, **the *Survey on Experience and Best Practices in Response to COVID-19* ("the Survey"), was subsequently conducted in June and July 2021. The Survey focused on gathering information, relevant experiences, and best data protection practices from GPA members and observers, regarding the following four topics**, which were a consolidation of the aforementioned six privacy issues:

(1) Health passports;
(2) Health monitoring of incoming travellers and returning nationals;
(3) Contact tracing measures; and
(4) Handling of children's or students' data in e-learning technologies.

6. **A total of 32 returns were received from GPA members and observers for the Survey, which formed the basis of the compilation of this *Part II of the Compendium of Best Practices in Response to COVID-19*.** The geographical distribution of the responses received was as follows:

Continent	Frequency	Percentage
Africa	2	6%
Asia	5	16%
Europe	18	56%
North America	5	16%
Oceania	2	6%
(Total)	**32**	**100%**

Figure 1: Geographical distribution of the responses to the Survey on Experience and Best Practices in Response to COVID-19.

7. The following is a digest of the 32 responses from members and observers of GPA on each of the four topics.

(1) Health passports

8. With the COVID-19 pandemic receding in some regions and national vaccination programmes gradually rolling out in 2021, many countries and jurisdictions recovered from national lockdowns and resumed domestic activities. Cross-border/boundary travel also gradually resumed. The use of digital proof of health (also known as 'health passports', 'health codes', 'health passes', 'vaccine passports', etc., to be referred to as 'health passport' in the ensuing paragraphs) to allow people to enjoy freedom of movement within and across national borders has been gaining popularity.

9. **'Health passports' generally refer to digital solutions developed to evaluate individuals' COVID-19 infection risks by recording whether they have been (a) vaccinated against COVID-19, (b) received a negative test result or (c) recovered from COVID-19.** They usually aim at achieving two main purposes. The first is to facilitate cross-border/boundary travel. In many jurisdictions, use of health passport have generally become a border/boundary entry requirement or a condition for waiving quarantine requirements. The second main purpose is to facilitate domestic activities within jurisdictions, as the use of health passports may also be required for individuals to enter restaurants, and enjoy cultural or leisure facilities, etc. In this Compendium, other certificates in paper or digital form with similar effect was also covered. Apart from governments and health authorities, private organisations, such as multinational technology companies, airlines, and non-profit organisations, have also developed health passports or similar initiatives to be used in the commercial context. While health passports may facilitate the reopening of borders/boundaries and recovery of economies,

they may also involve heightened privacy risks due to potential mass scale pooling and sharing of health data across borders/boundaries and across a range of entities, as well as discriminatory effects against those who, for clinical reasons or other reasons, may be unable obtain the passports..

Prevalence of Health Passports

10. **The Survey showed that health passports were commonly used by different jurisdictions for cross-border/boundary travels and domestic activities.** Among the 32 DPAs that responded to the survey, **21**[1] **(66%) stated that their jurisdictions had health passports for cross-border/boundary travel.** However, it is worth noting that 15 out of the 21 jurisdictions (71%) which have implemented cross-border/boundary travel health passports adopted the EU Digital COVID Certificate gateway developed by the European Commission in June 2021. Another nine DPAs (28%) stated that health passport initiatives for cross-border/boundary travel purposes were under consideration by their governments. Only two DPAs (6%) responded that they did not have a health passport for cross-border/boundary travel, nor was one under consideration or in development.

11. On the other hand, **17 (53%) of the DPAs also stated that their jurisdictions had health passports for facilitating domestic activities.** Another seven DPAs (22%) stated that health passport initiatives for facilitating domestic activities were under consideration by their governments. Only eight DPAs (25%) responded they did not have a health passport for facilitating domestic activities, nor was one under consideration or in development.

Categories of Health Passport	**Number of Jurisdictions**
Jurisdictions implemented health passports for facilitating cross-border/boundary travel	21 out of 32 (66%)
Jurisdictions implemented health passports for facilitating domestic activities	17 out of 32 (53%)

Figure 2a: Adoption rate of health passports

[1] For consistency in the results, although the EU Digital COVID Certificate is not for travelling outside of the EU, and is classified by the European Data Protection Supervisor ("the EDPS") as a health passport for domestic purpose in its return, the return by the EDPS was counted as for cross-border/boundary purpose for this Compendium. Similarly, in Newfoundland and Labrador (Canada), a travel form is required for people entering the province from other parts of Canada. Although the travel form is not for travelling outside of Canada, and is classified as a health passport or facilitating domestic activities in the return submitted by Office of the Information and Privacy Commissioner of Newfoundland and Labrador, it is counted as for cross-border/boundary purpose for this Compendium.

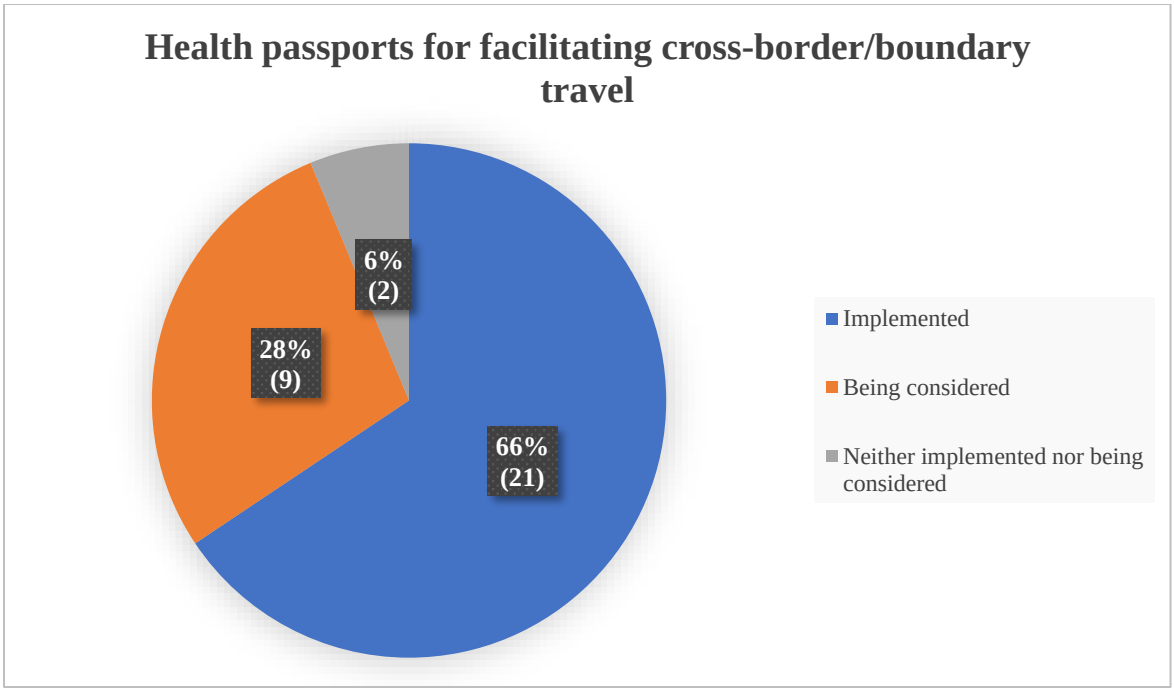

Figure 2b: Adoption rate of health passport for facilitating cross-border/boundary travel

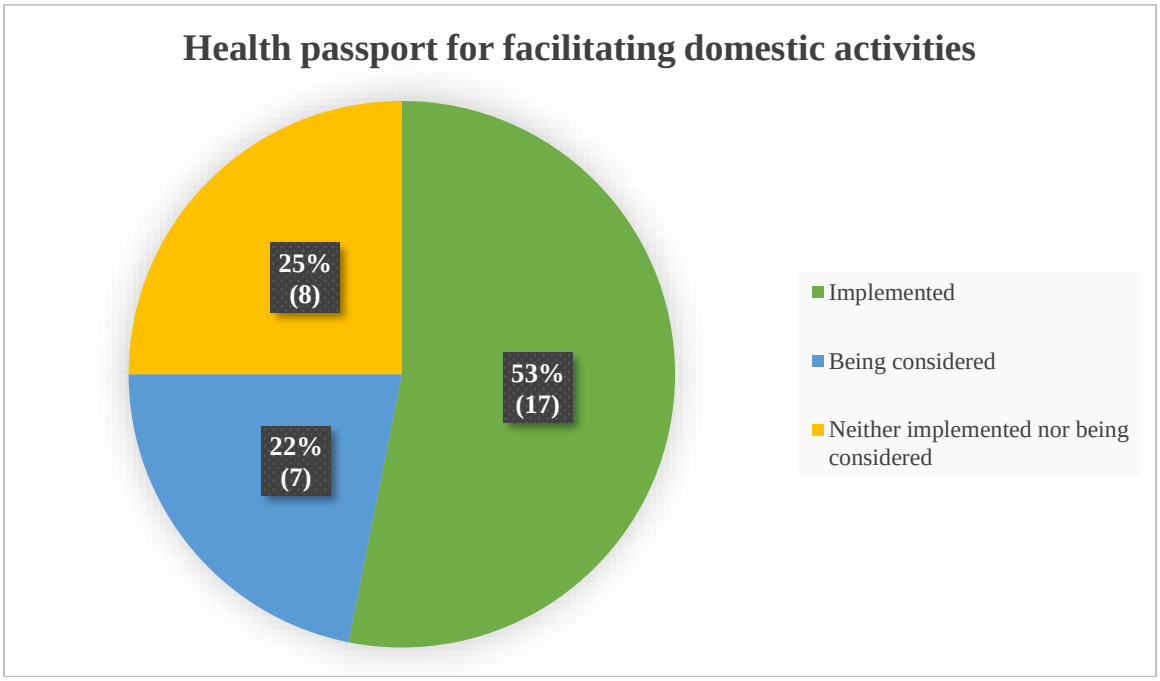

Figure 2c: Adoption rate of health passport for facilitating domestic activities

Perceived public acceptance

12. The DPAs were asked to rate from 1 to 5 the public's acceptance of 'health passport' as perceived in their respective jurisdictions from the perspective of personal data privacy, a rating of 1 being the least receptive and 5 being the most

receptive. Several DPAs indicated that as health passports were still in early stages of implementation, insufficient information on public acceptance was available. **Among 19 out of 32 (59%) who were able to give a rating, the average rating was 3.79, and 4 was the most frequent rating. Out of these 19 DPAs, 11 (58%) gave a rating of 4 or 5. This indicated that the majority of the DPAs perceived that health passports were generally well received by the public at this time of the pandemic.**

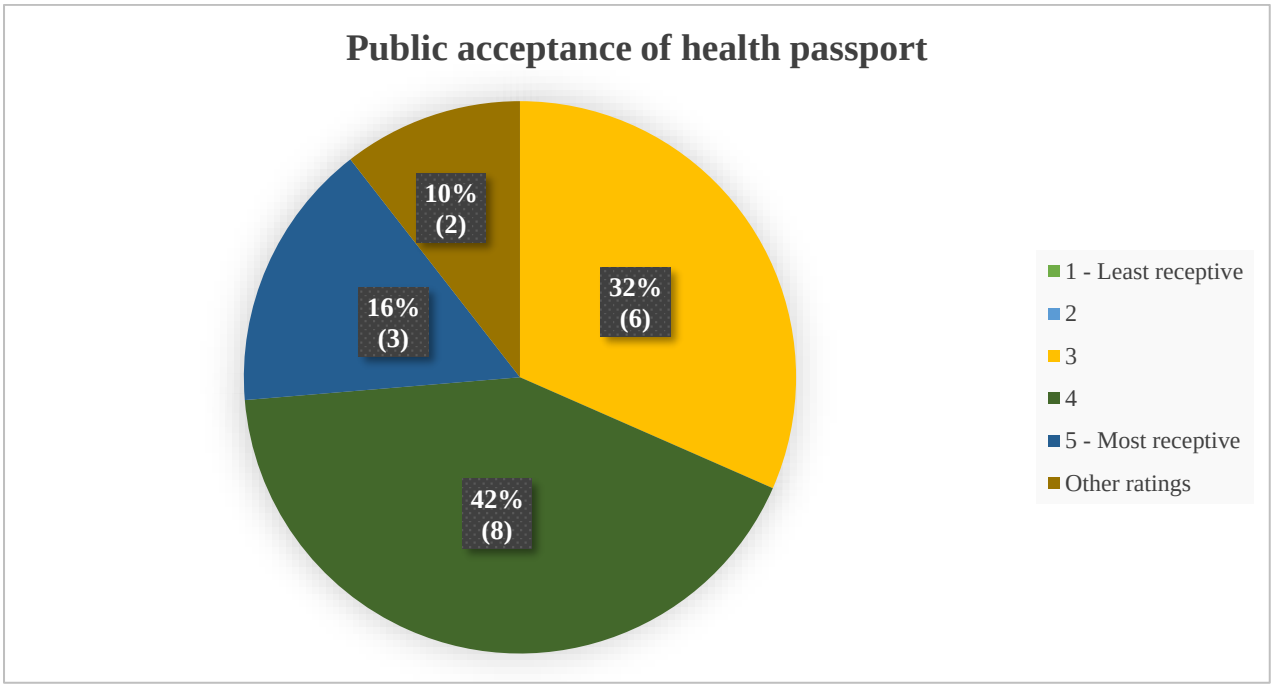

Figure 3: Public acceptance of health passport [2]

Modus operandi of health passports

13. The 'health passports' initiatives reported in the Survey, for either cross-border/boundary travel or domestic activities, often entailed requirements for disclosing and presenting certain information or proof at borders/boundaries and/or upon entry of selected premises. **Many health passports generated a digital proof, usually in a machine-readable QR code, by retrieving personal data and health information in relation to COVID-19 from centralised health records or provided by individuals.** The digital proof could then be presented and verified upon entry to another jurisdiction or a domestic venue. On the other hand, many DPAs also indicated that their health passports could be carried in paper form, such as the EU Digital COVID Certificate.

[2] Two DPAs gave a rating of between 3 and 4. Their ratings were classified as 'other ratings'.

14. Moreover, some jurisdictions, such as Canada (federal), Hong Kong, China and Macao, China reported that online declaration forms were used to gather relevant personal data and health information of individuals, then a 'receipt' may be generated from the online form as a condition for entry. On the other hand, for facilitating domestic activities, some jurisdictions such as Gabon and Mauritius may simply require an individual to show a vaccination proof, such as a vaccination card.

Personal data collected in health passports

15. Many of the aforementioned health passports commonly collected and processed personal data such as name, data/year of birth, identification numbers/documents, as well as contact information such as telephone number. Some health passports also collected self-reported COVID-19 symptoms. **Generally, many of the digital certificates in health passports are generated based on information regarding whether individuals have vaccinated against COVID-19, tested negative with COVID-19, and/or recovered fully from COVID-19.** For example, the name, time and location of the vaccination shot received or the COVID-19 test conducted were included. Some digital certificates would also contain unique identifiers, as well as information regarding the issuing organisation of the certificates.

Legislative changes

16. **The survey showed that many jurisdictions had introduced legislation to facilitate the implementation of health passports.** Notably in the EU, the European Commission launched and approved in June 2021 an EU-wide regulation providing for the creation and implementation of an EU Digital COVID Certificate. The regulation required all EU Member States to use the EU Digital COVID Certificate framework and issue certificates for the purpose of facilitating the exercise of the right to free movement within the EU during the COVID-19 pandemic. Several DPAs stated that their jurisdictions also introduced similar legislation. For example, both San Marino and Switzerland passed law to regulate the issuance of health passports in their respective jurisdictions. Italy introduced the 'Italy Reopens' decree to enable the use of health passport for travelling between Italian regions and other domestic activities. Hong Kong, China, introduced regulations regarding the information required to be provided by individuals for entering borders/boundaries and certain business and public premises in Hong Kong, China.

Privacy considerations for health passports

17. Owing to the apparent privacy risks arising from the implementation of health passports, **15 out of 32 (47%) of the DPAs stated that they were involved in the development process of their health passports.** The roles of the DPAs included reviewing the Data Protection Impact Assessment ("DPIA") or Privacy Impact Assessment ("PIA") of the initiatives, or providing advice to their respective governments. Several DPAs, such as those of New Zealand, UK and Canada (federal and provincial) published public statements or blog posts in regard to their views on the health passport initiatives, way before their implementation. On the other hand, some DPAs, such as the European Data Protection Supervisor, the DPA of Czech Republic and the DPA of Italy, criticised that insufficient assessment of privacy risks and consultation had been conducted by the authorities during the development of health passports.

18. Among the 23 jurisdictions which had introduced health passports, 12 (52%) jurisdictions stated that a DPIA or PIA was conducted. **Examples of the privacy risks reported in those assessments or otherwise observed by DPAs themselves are as follows (non-exhaustive):**

    a. Data security risks, including data breaches or other cyberattacks;
    b. Forgery of health passports;
    c. Unnecessarily displaying or sharing of personal data during the use of health passports;
    d. Personal data being retained for longer than necessary; and
    e. Personal data being reused for secondary usage, i.e. 'scope creep' or 'mission creep'.

19. There were also concerns about non-privacy risks, such as discrimination against those without the means to use health passports, and normalisation of health surveillance after the pandemic.

Data Protection principles and best practices

20. Owing to the fact that health passport initiatives have been rapidly developing worldwide by both public and private sectors since the beginning of 2021, there was an urgent need for the Working Group to provide relevant guidance on data protection in this regard. Therefore, the Working Group agreed in January 2021 that a public statement on the issue should be published as soon as possible.

Consequently, the Information Commissioner's Office (ICO), UK spearheaded the drafting of the public statement together with other members of the Working Group. The public statement was adopted by the GPA Executive Committee and published as the GPA Executive Committee joint statement on the use of health data for domestic or international travel purposes (Joint Statement) on 31 March 2021.

21. The Joint Statement recommended governments and other organisations to consider and pay due regard to a set of data protection principles when processing health data for the purposes of cross-border/boundary travel, in order to build trust and confidence with the public. These principles were largely consistent with the data protection principles recommended by DPAs in the Survey. **Below is a consolidated list of the principles that were advocated in the Joint Statement and by the DPAs that responded to the Survey.**

    a. **Privacy by Design**: embedding 'Privacy by Design and Default' principles into the design of health passports or similar measures, such as by conducting a formal and comprehensive assessment of the privacy impact on individuals before the commencement of any processing (e.g. through conducting a DPIA, consulting DPAs);

    b. **Data minimisation**: collecting the minimum health information from individuals or other sources that is necessary for implementing health passports;

    c. **Retention limitation**: consider carefully for how long data should be retained, and design a retention schedule for the safe deletion of information once it is no longer required;

    d. **Purpose specification**: clearly defining the purpose for the collection, use and disclosure of personal data, i.e. for alleviating the public health effects of COVID-19. Personal data must not be used in a manner incompatible with the specified purpose;

    e. **Necessity, proportionality, and lawful basis**: health passports should be operated with a lawful basis, and health data should only be processed if and when it is necessary and proportionate to do so. There should be sunset clauses for the use of health passports and to delete personal data collected permanently once the pandemic ends;

    f. **Fairness**: the data protection rights of those who may not be able to use health passports or have access to electronic devices must be protected, and alternative solutions (e.g. paper-based certificates) should be considered to ensure that such individuals do not suffer from discrimination;

g. **Accuracy**: personal data, including vaccination status and COVID-19 test results, shall be accurate and up to date;

h. **Data security, integrity and confidentiality**: fully assessing the cybersecurity risk of digital systems or apps, taking full account of the risks that can emerge from different actors in a global threat context; protect personal data in health passports against unlawful or accidental access, processing, alteration, loss, destruction or damage, etc; and

i. **Openness**: being transparent and making available to individuals about the data protection policies and practices in relation to the use of health passports.

22. Good data protection practices were either recommended by DPAs, or already adapted in their jurisdictions in the implementation of health passports to give effect to the principles mentioned above. **Some common good practices are summarised below:**

a. Minimising personal data collection by not actively tracking or logging individuals' activities through the health passport mobile apps, and not creating a new central database that pools together health data from health passports;

b. Minimising the personal data disclosed while displaying the digital certificate or testing/vaccination records in health passports, such as by (i) providing checks on the basis of scanning the barcode/QR code so as to restrict the amount of personal data displayed; (ii) partially masking the name and identification number of the individual if possible; or (iii) providing a data minimised alternative version of health passport for domestic use in contexts where individuals need not disclose the full details of their valid certificate;

c. Minimising transfer of personal data to third-parties (e.g. premise operators, border authorities of countries visited) by building the app in such a way that the status of the individual can be verified without any transfer of personal data, such as in the case of the EU Digital COVID Certificate. Privacy preserving solutions such as federated identity systems and device level processing can also be considered;

d. Implementing measures to strengthen data security, such as (i) ensuring and verifying the authenticity of digital certificates through cryptographic means; (ii) storing the digital signature of certificate issuing bodies in secure national databases; (iii) deleting the personal data collected upon expiry of the relevant certificate; (iv) preventing unofficial third party applications from reading the data stored in the digital certificates;

e. Building privacy safeguards through legal means, including specifying the purposes for which health passports are allowed for use, and the planned timeline for reviewing the continuing necessity of the health passports. Setting in place regular reviews or audits for health passport initiatives;

f. Pledging to decommission the health passport no later than a specific date, as well as to prohibit access to and subsequent use of personal data once the pandemic has ended, to prevent scope creep in the long run;

g. Being open and transparent by (i) making the source code and technical specifications of the software publicly available and demonstrating that no backdoors were implemented; (ii) disclosing the list of entities which might have access to the personal data; and

h. Providing the choice of having the health passport certificate in paper form and not obligating the use of an electronic device.

(2) Health monitoring of incoming travellers and returning nationals

23. Even during the height of the pandemic, many borders/boundaries were not completely shut down. Countries or jurisdictions have allowed certain travellers and returning nationals to enter, on condition that their health status in relation to COVID-19 must be reported and monitored. There were inherent privacy concerns in such measures, as this often involved collection of health data upon arrival as well as continuous monitoring of individuals afterwards for a period of time.

Legal requirements

24. **Twenty-six out of 32 (81%) of the DPAs stated that their jurisdictions had health monitoring measures and requirements in place for incoming travellers and returning nationals.** Some other provincial or supranational jurisdictions reported that they were not in the position to discuss national requirements.

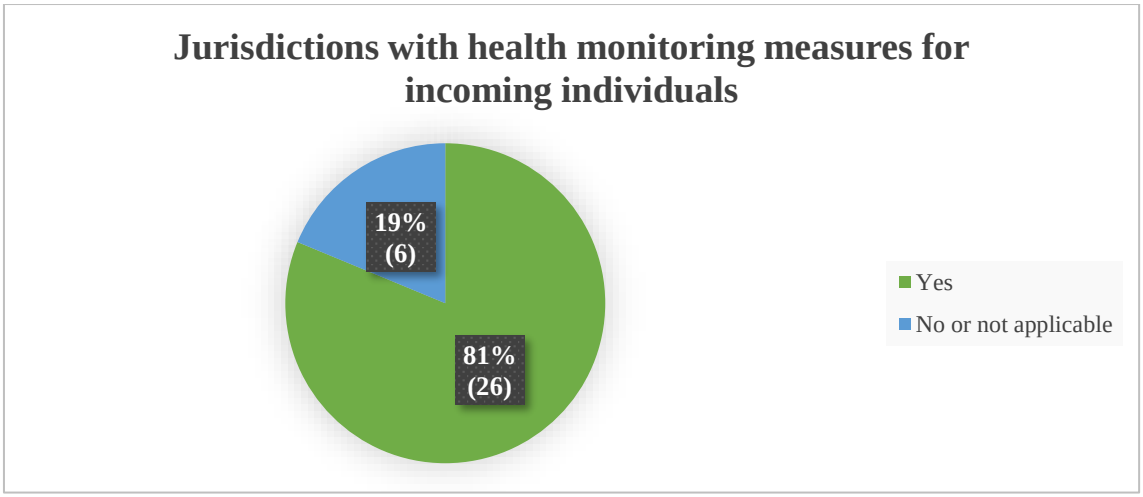

Figure 4: Jurisdictions with health monitoring measures for incoming individuals

25. To prevent incoming individuals from bringing in and spreading the COVID-19 virus, collection of personal health data and health monitoring during mandatory quarantine were commonplace requirements for incoming individuals. In terms of collection of personal data, it was not surprising that COVID-19 testing result was the most often collected item, either upon arrival in the form of a testing certificate, or afterwards from individuals by conducting further testing, say, in 3 or 5 days upon arrival. Data regarding COVID-19 testing results may be collected multiple times from individuals during their quarantine. The other commonly collected personal data for health monitoring purposes was COVID-19 related symptoms reported by individuals, followed by body temperatures of the individuals. It was also stated in several responses that some jurisdictions required individuals to complete declaration forms, requiring details such as travel history, vaccination records and contact details to be reported, which could potentially be used to facilitate domestic contact tracing activities by public health authorities.

26. In addition, according to information provided by several DPAs, for example, from Georgia, Hong Kong, China, and Japan, incoming individuals might be required to use electronic devices and install mobile applications for monitoring of their health during quarantine. This included apps developed for purposes such as enforcing mandatory quarantine requirements, facilitating the conducting of tests and obtaining of test results, as well as assisting contact tracing efforts.

Privacy risks

27. According to the DPAs' experiences reported in the Survey, **the common privacy risks in relation to health monitoring of incoming travellers and returning nationals were as follows (non-exhaustive):**

a. Unnecessary collection, access and retention of personal data, e.g. archiving of individuals' temperature through storing video footage, setting up of central registers;

b. Doubt on data accuracy of personal health data provided by incoming individuals;

c. Surveillance and intrusion to individuals' privacy when ensuring their compliance with quarantine requirements;

d. Lack of voluntary consent for the provision of personal data by incoming individuals;

e. Unauthorised secondary use and sharing of personal data and health data of quarantined persons; and

f. Data security risks, e.g. (i) sensitive data of incoming individuals may be prone to unauthorised access and disclosure, (ii) lack of accountable access control in electronic systems used to process health data of incoming individuals.

Best Practices

28. **Best privacy practices as recommended or observed by DPAs in regard to health monitoring of incoming travellers and returning nationals are as follows (non-exhaustive):**

a. Ensuring that there are legal bases for collecting, processing and storing personal data from incoming individuals;

b. Being transparent to incoming individuals regarding the collection and processing of their personal data, such as by providing at the borders verbal and written notices on the collections, uses and disclosures of their personal data;

c. Setting a conservative time limit for the retention of personal data collected, such as a period that is necessary for contact tracing activities to be carried out;

d. Minimising the data collected from incoming individuals to only what is necessary for health monitoring, for example, (i) use alternative methods to confirm individuals' compliance with quarantine requirements, e.g. ascertaining that an individual under quarantine has not left the designated place by analysing environmental signals, rather than location tracking

during the quarantine period; (ii) no unnecessary archiving of video footage or temperature screening at borders;

e. Prohibiting unauthorised disclosure and publication of personal data of infected persons, anonymising / de-identifying and aggregating such personal data where possible, to avoid possible future misuse and discrimination;

f. Implementing adequate data security measures in the systems containing the personal data of incoming individuals collected for health monitoring purposes, such as (i) enabling two-factor authentication for access; (ii) providing the access to personal data to staff through individual accounts, instead of blanket access using shared accounts in order to prevent undetected or unauthorised access; and

g. Enhancing the accountability of data users / controllers (e.g. health authorities) by (i) clearly limiting the health monitoring measures to the purpose of fighting the current COVID-19 pandemic only; (ii) designating responsible persons for administering health monitoring measures such as temperature screening; (iii) having data sharing agreements between government authorities (e.g. border authorities, health authorities, other authorities involved in contact tracing activities) to ensure that personal data was shared and used lawfully and properly.

(3) Contact tracing measures

29. Contact tracing plays an important role in fighting the COVID-19 pandemic. Digital contact tracing measures, such as contact tracing mobile applications, have been developed by governments to allow health authorities to swiftly identify close contacts of infected persons. Privacy risks of contact tracing measures was a topic explored in Part I of the Compendium, and contact tracing apps was a hotly debated subject in 2020. Key privacy issues included whether the contact tracing apps were built using a centralised[3] or decentralised[4] approach. In this Part II of the Compendium, the goal of re-exploring this topic was to examine how the discussion on the topic and the good data protection practices regarding the use of contact tracing apps have evolved over the past year.

30. **Twenty-one out of 32 (66%) of the DPA stated in their responses that their jurisdictions had implemented a mobile application for contact tracing**

[3] For contact tracing apps adopting a centralised approach, personal data of users is collected and stored in a central database upon registration. Often, anonymised proximity data collected by the apps will be uploaded to central servers when the users become infected, thus allowing the relevant authorities to trace their close contacts.

[4] In a decentralised approach, registration is usually not required. Anonymised proximity data collected by the apps would remain on the users' mobile devices. Only the pseudonym IDs of the infected users assigned by the app will be uploaded to central servers in order to notify those who may have been exposed to the virus.

purposes. Another 2 DPAs (6%) stated that one was under consideration by their governments. Compared to last year where 72% of the respondents stated that they had implemented a digital contact tracing app, the prevalence of contact tracing apps has been maintained at a similar level (albeit the pools of respondents in the two Compendiums are not identical). **Among the 21 jurisdictions with contact tracing apps, 18 of them stated that their contact tracing app used a decentralised approach** (often referred to as an exposure notification app), 15 of which at least partly employed the exposure notification API jointly developed by two tech giants (i.e. the Google-Apple Exposure Notification API), and the other three out of the 18 apps were reported to have used other decentralised approaches. **Two other apps used a centralised approach[5].**

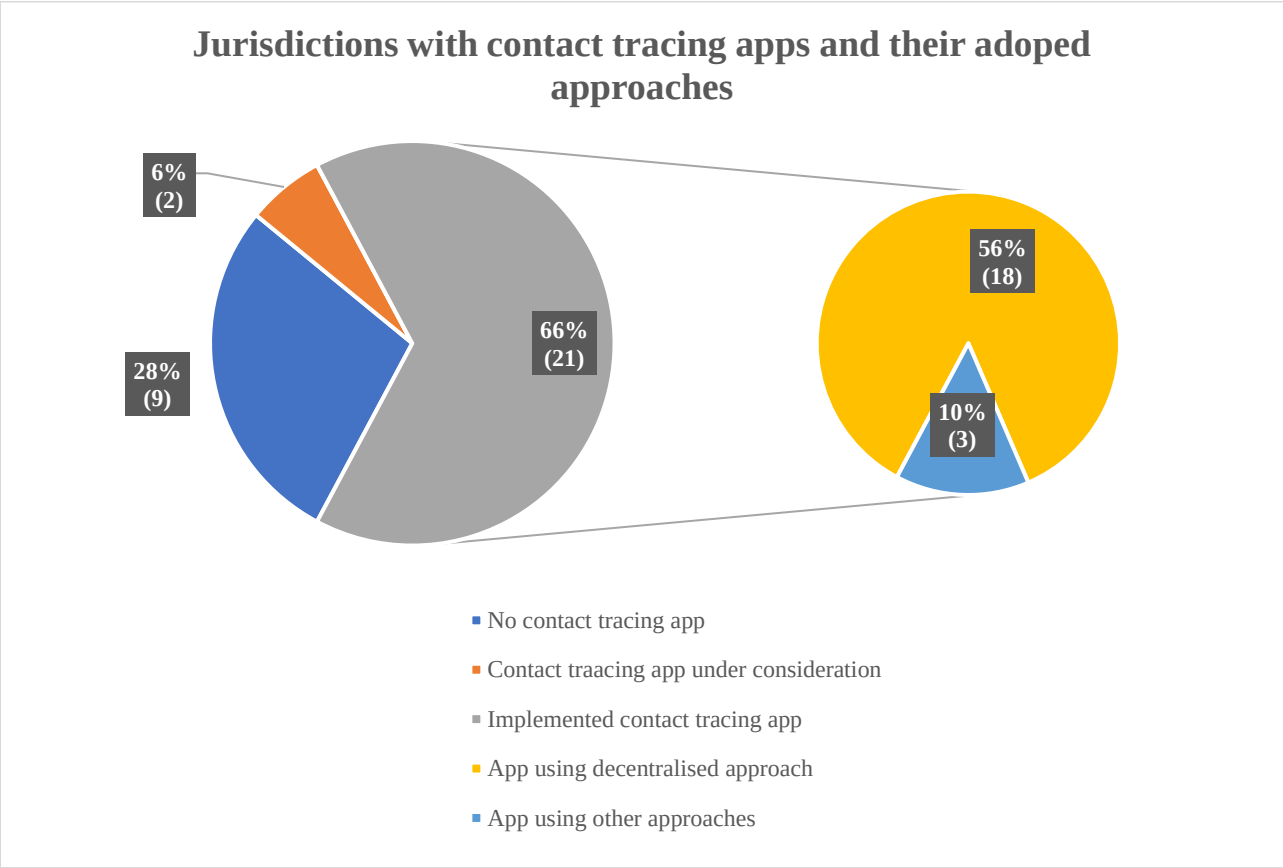

Figure 5: Jurisdictions with contact tracing apps and their adopted approaches

31. **In terms of the underlying technology of the contact tracing apps, most employed the Bluetooth function of mobile devices (e.g. the apps built solely on the Google-Apple Exposure Notification API) to record contacts between individuals by way of Bluetooth signal exchange,** while several apps combined Bluetooth with other data sources such as GPS location data and mobile network data. A few contact tracing apps, such as those of in Hong Kong, China and

[5] The approach used in the only remaining contact tracing app reported was unknown.

Victoria, Australia, recorded visits to premises by scanning QR codes instead of using Bluetooth technology.

Legal requirements

32. **Twelve out of 32 (38%) of the DPAs stated that legislation was introduced or amended to facilitate contact tracing.** Some of the laws aimed at addressing the specific privacy concerns arising from the implementation of contact tracing apps and at strengthening personal data protection around their development and use. For example, the relevant laws in Switzerland, Italy and Malta's contained provisions setting out privacy-protecting principles and standards, which in turn facilitated privacy by design in the development and use of their national contact tracing apps. On the other hand, some of the jurisdictions, including Hong Kong, China, Gibraltar and the UK, facilitated contact tracing by, for example, explicitly requiring certain premises (e.g. restaurants, hospitals) to collect personal data, such as contact information, from their customers and visitors.

Privacy assessment and risks

33. Among the 21 jurisdictions with contact tracing apps, 18 (86%) of them stated that a DPIA or PIA was conducted before implementation of the apps. This indicated that the awareness of the potential privacy and data protection risks of contact tracing apps have been high.

34. **Major privacy risks identified by the DPAs regarding the use of contact tracing apps were as follows (non-exhaustive):**

    a. Data security related risks, arising from (i) longer than necessary data retention, (ii) potential data breaches and cyberattacks compromising sensitive personal data, and (iii) malicious access to backend databases;

    b. Privacy risks in relation to the use of Bluetooth technology, such as potential bugs and vulnerability in the systems and the building of social graphs by scanning Bluetooth signals in open places;

    c. Re-identifying individual users of the app by using, for example, user IDs, IP addresses and other metadata;

    d. Collecting more personal data than necessary for the purpose of contact tracing, such as the tracking of individuals' movements, collection of location data, and revealing information about individuals' usage of the apps and devices;

e. Unauthorised processing and disclosure of sensitive data in the apps, especially in relation to individuals tested positive with COVID-19; and

f. Using the apps and the contact tracing data for unrelated purposes, resulting in mission creep in the long run.

Best practices and the way forward

35. The best practices emerged from Part I of the Compendium to address the privacy concerns arising from contact tracing apps were largely consistent with the best practices suggested in the responses received this year. **Below is a combination of best practices received among the two years (non-exhaustive):**

a. Conducting DPIA or PIA before rolling out the contact tracing apps and regular audit and reassessment thereafter to ensure Privacy by Design;

b. Permitting voluntary use of contact tracing apps;

c. Adopting data minimisation techniques such as (i) collecting only anonymous/pseudonymised/de-identified data (e.g. no name, phone number, or location data would be collected by the apps), and (ii) uploading only the information of infected persons to central databases (i.e. decentralised exposure notification), which was usually also done anonymously;

d. Implementing anonymisation and other security measures to mitigate the risk of re-identification, such as through (i) using anonymous identifiers or keys that regenerate regularly so that it is less susceptible to hacking or malicious re-identification; (ii) being extra cautious in the collection and storage of metadata such as IP addresses of individuals;

e. Adopting various measures to demonstrate transparency and enhance public trust, such as (i) publishing privacy policies of the contact tracing apps; (ii) informing the users when their data is deleted; and (iii) chartering the DPAs or oversight committees to review the operation of the apps; (iv) limiting the use of personal data for contact tracing purposes by way of legislation or other means; (v) informing users the operation of the algorithms used to assess the exposure risk in the app;

f. Spelling out the retention periods for the data collected by contact tracing apps. Common retention period ranged from 14 to 30 days after collection; and

g. Pledging that the contact tracing apps would be scrapped when the COVID-19 pandemic is over. For example, the federal app in Canada would shut down within 30 days of health authorities declaring so. In Italy, it was

required by legislation that the use of contact tracing app would be terminated by 31 December 2021, and all personal data processed must be deleted or made anonymous after that date.

36. At this stage of the pandemic, besides best practices regarding the development and implementation of contact tracing apps, **some DPAs considered that it is opportune to explore and highlight good practices in regard to interoperability, efficacy and effectiveness of contact tracing apps.** For example, in terms of interoperability, the European Data Protection Supervisor expressed that they had called for a pan-European approach to contact tracing apps, and the European Commission has set up an EU-wide gateway to ensure interoperability across contact tracing apps of member states. This was adopted by, for example, the apps in Germany, Italy, and Malta. Such regional interoperability may also provide more freedom to people's movements and remove travel restrictions during times of recovery.

37. In terms of efficacy and effectiveness, many DPAs agreed that assessing and regularly reviewing the efficacy and effectiveness of contact tracing apps would be a good example of data protection practice. (This follows the rationale that if a contact tracing app is not effective, its use will not be necessary and proportionate even if it is not privacy intrusive.) Indeed, multiple studies have emerged in different jurisdictions regarding the impact of contact tracing apps on infection rates and preventing spread of the virus. **While there were criticisms against contact tracing apps having low uptakes, overwhelming individuals with exposure notifications and failing to help contain outbreaks[6], the apps were also seen as effective and helpful by some.** For example, research have suggested that contact tracing apps with a low adoption rate would still be useful to some extent, although the higher the level of uptake of contact tracing apps, the more effective it would be in detecting community infections[7]. An evaluation study on the UK contact tracing app has demonstrated that for every 1% increase in app users, the number of infections can be reduced as much as 2.3%[8]. Furthermore, a review of the Germany contact tracing app revealed that around 6% of the COVID-19 tests carried out as a result of a warning from the contact tracing app were positive, which is comparable to that from analogue contact tracing[9]. Future

[6] Algorithm Watch (2021). Digital contact tracing apps: do they actually work? A review of early evidence: https://algorithmwatch.org/en/analysis-digital-contact-tracing-apps-2021/ ;
Alt Advisory (2021). The Covid Apps Project - South Africa Country Report: https://altadvisory.africa/2021/05/05/the-covid-apps-project/
[7] MIT Technology Review (2020). *No, coronavirus apps don't need 60% adoption to be effective*: https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/
[8] The Alan Turing Institute (2021). *Demonstrating the impact of the NHS COVID-19 app:* https://www.turing.ac.uk/blog/demonstrating-impact-nhs-covid-19-app
[9] Corona Warn-App Open Source Project (2021). *About the Effectiveness and Benefits of the Corona-Warn-App*:

exploration on contact tracing apps can further focus on this aspect when more comprehensive evidence comes to light.

(4) Handling of children's or students' data in e-learning technologies

38. Children's privacy has always warranted more protection due to their vulnerability, especially when it comes to online activities. As a result of social distancing measures during the pandemic, many schools have migrated their teaching environment from offline to online to enable children to continue learning. Videoconferencing software and online learning platforms have been widely used, possibly resulting in increased collection of personal data and heightened online privacy risks for children and students.

39. **DPAs responded that they observed either a significant (21 out of 32, 66%) or moderate (4 out of 32, 12%) increase in the use of e-learning technologies during the COVID-19 pandemic.** According to the Survey, schools in many jurisdictions leveraged videoconferencing and virtual classroom software, as well as government-developed online learning platforms, as their main technological tools for e-learning.

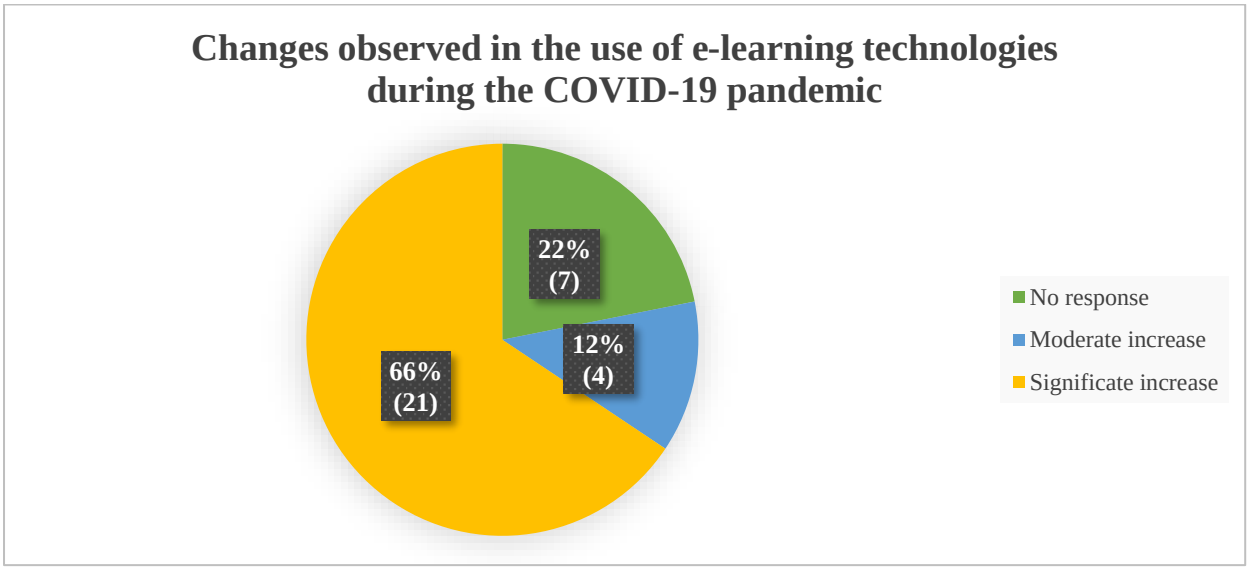

Figure 6: Changes observed in the use of e-learning technologies during the COVID-19 pandemic

https://www.coronawarn.app/en/science/2021-06-15-science-blog-1/

Privacy risks

40. In terms of assessment of privacy risks, 16 out of 32 (50%) of the DPAs would recommend that a DPIA or PIA be conducted prior to the adoption of e-learning technologies by education institutions, even if it may not be a legal requirement to do so in some jurisdictions. This is because education institutions adopting e-learning technologies were likely to result in a high risk to individuals including children and students, according to some responses.

41. **Major privacy risks identified in this context were mostly related to the use of videoconferencing tools and the fact that children are more vulnerable, for example (non-exhaustive):**

    a. Children's ability to give meaningful consent depends on their individual evolving capacities as well as the clarity of the information being provided to them about their choices and the context. In many cases, young children may not be able to give meaningful consent for the collection of their personal data, since they may not have the capacity to fully comprehend the information provided to them regarding the processing of their personal data and the privacy settings of the e-learning tools. They may also be incapable of assessing what kinds of personal data may be unnecessary for using the e-learning tools;

    b. Intrusion to children's privacy and homelife via use of videoconferencing tools, for example (i) overcollection of children's personal data while conducting virtual lessons, especially when the use of camera by students was made compulsory, or no background blurring / masking function was available; (ii) unauthorised or inadvertent collection, use, processing and distribution of audio, photos and videos, which may be considered sensitive biometric data of students; (iii) remote monitoring of students' attendance and behaviours during lessons and exams, which may involve using facial recognition technologies;

    c. Lack of management framework or measures in e-learning tools that are proportionate to the volume and sensitivity of children's personal data involved;

    d. Cross-border/boundary transfer of children's personal data arising from the use of e-learning tools as personal data might be stored in servers located in other jurisdictions;

    e. Data security related risks, including (i) risk of students' accounts being compromised due to account theft, lack of appropriate security software and

strong passwords, etc.; (ii) security risks of videoconferencing software such as online classes not being end-to-end encrypted, and unauthorised invasion to the virtual meeting rooms potentially exposing children to unwanted and inappropriate content; and

f. Children's personal data collected in e-learning tools being used for marketing and profiling purposes, the risks and consequences of which may be unknown to the children themselves.

Best Practices

42. Privacy concerns in relation to the use of e-learning technologies by children are clearly considered significant by many DPAs. Among the 32 DPAs, 14 (44%) stated that they had issued guidance on the topic to provide relevant advice to educational institutions. Many DPAs issued guidance specifically targeting schools / teachers, and parents / children separately.

43. **Some examples of good data protection practices for schools and teachers, in regard to the use of e-learning technologies, suggested by DPAs or adopted in various jurisdictions, are detailed below (non-exhaustive):**

a. Conducting a DPIA or PIA before using e-learning technologies that process children's personal data. Schools' privacy and security practices in the use of e-learning technologies should be reassessed and audited regularly thereafter;

b. Strictly adhering to the principle of data minimisation, in view of the inherent vulnerability of children, and especially given that children may not possess the capacity to provide consent to the collection of their personal data. For example, (i) students should not be requested to turn on their cameras during the whole of the lessons; (ii) schools should disable online tracking or recording functions of e-learning tools; (iii) recording of lessons and the subsequent use of the footages should only be for specific purposes such as allowing students who had missed the lesson to catch-up, and should be deleted as soon as the purposes have been fulfilled;

c. Having a lawful basis for collecting and using children's or students' personal data. It would be a good practice to obtain express consent of the students or their parents beforehand, even if it is not a legal requirement;

d. Assessing the data protection practices of e-learning tools before adopting them. For example, (i) consider whether the tool store activity logs, the length of the time personal data will be stored, whether data subjects rights would be ensured, whether personal data of teachers and students would be collected

by third-parties such as the software developers; (ii) if cloud services are involved, consider and assess the security of storing personal data in clouds, and ensure that any transfer of personal data to servers in other jurisdictions is lawful;

e. Implementing robust data security measures for e-learning platforms and videoconferencing tools. For example, (i) ensuring any school assignments and documents are transmitted through secure channels and not through public or social media platforms; (ii) safeguarding teachers' and students' accounts by requiring strong passwords; (iii) keeping the operating systems of e-learning tools up-to-date; (iv) taking steps to protect the school's information systems and network from cybersecurity risks such as virus, malware, spyware etc.;

f. Enhancing the school's accountability in the use of e-learning technologies, for example, by (i) setting internal policies to regulate the collection, retention, use, sharing and deletion of children's personal data (e.g. regarding the recording of audio and video of lessons); (ii) reviewing regularly data processing by teachers; (iii) devising plans to deal with data breaches, incidents of loss of devices or stolen accounts; (iv) keeping records on the use of e-learning tools, including the reasons that the specific tools or platforms were selected, the roles and responsibilities of different staff, and the decisions to collect students' personal data;

g. Teachers or staff conducting online lessons should adopt good practices on the use of videoconferencing tools. For example, (i) using unique meeting ID and password for each online class to prevent uninvited participants; (ii) avoid disclosing meeting details publicly or to parties other than students and their parents; and

h. Communicating and being transparent with parents and guardians, for example, by (i) providing them in advance the schools' online privacy policies; (ii) providing guidance about how to customise privacy settings of their children's accounts.

44. Furthermore, **examples of good data protection practices for parents, guardians and children, in regard to the use of e-learning technologies, suggested by DPAs or adopted in various jurisdictions, are detailed below (non-exhaustive):**

a. Children should refrain from indiscriminately collecting and sharing pictures and videos, or other personal data, of other meeting participants during the lessons without their consent;

b. Children should only use designated official software for e-learning purposes, and parents should ensure that only software downloaded from official websites of the developers are used by their children;

c. Parents should protect their children's privacy and minimise disclosure of personal data and details, such as by enabling virtual background options during lessons;

d. Parents should enhance the security of their children's accounts of e-learning tools by (i) using different email addresses to register for different platforms and tools; (ii) adopting strong and unique passwords for all accounts; (iii) activating enhanced security features such as multi-factor authentication; and

e. Parents should educate their children about the importance of personal data privacy as well as respecting other's personal data privacy.

Work of the sub-group on regulatory capacity building

45. Apart from the best practices collected by the sub-group on emerging privacy issues through the *Survey on Experience and Best Practices in Response to COVID-19* as detailed above, the other sub-group of the Working Group on regulatory capacity building also conducted the *COVID-19 Protocols Lessons Learned Survey* among non-regulatory organisations in early 2021 to gather insights regarding the impact of the pandemic on regulatory capacity.

46. As part of the response to COVID-19, a significant amount of personal health information has been collected and shared by employers, businesses, schools, insurance companies, healthcare providers and government agencies. In order to properly understand how well-equipped these organisations were for handling personal data in volumes and ways they have not experienced before, the sub-group on regulatory capacity building sought views from individuals and organisation representatives about their data processing practices and how regulators could have done better in addressing the privacy issues arising from the pandemic, among others. The survey can be viewed here: https://survey.alchemer.com/s3/6191656/Global-Privacy-Assembly

47. The primary thematic areas reviewed in this survey included the following:

a. Communications and guidance from regulators;
b. Organisational/operational impact of COVID-19 restrictions on data subjects' rights;
c. Data sharing, data security and data breach reporting;
d. Privacy technologies development, framework and design; and
e. Supervision and enforcement.

48. The key findings of the survey were set out in the Regulatory Capacity Lessons Learned Report at Annex B of this Compendium. The survey results were also presented by the DIFC Commissioner's Office and the Jersey Information Commissioner's Office at a webinar jointly hosted by the GPA and the Centre for Information Policy Leadership in August 2021.

Concluding remarks

49. This Compendium collated the relevant experiences and best privacy practices regarding several emerging privacy and data protection issues in the context of the COVID-19 pandemic in the GPA community. The landscape of privacy protection during the pandemic is still rapidly changing, with innovative technological solutions and more challenging privacy issues constantly arising. For instance, one year ago, contact tracing apps dominated the discourse surrounding data protection and the pandemic; a year later, the use of health passports to facilitate global recovery from the pandemic have caught the attention of many DPAs.

50. As the world underwent this major public health crisis, a 'new normal' has emerged, and the data protection sphere is no exception. The DPA community, including the GPA, has responded constructively during this fast-changing period by continuously providing guidance and advice to governments and the public on many emerging privacy issues in a timely manner. Looking ahead, even if some pandemic prevention and protection measures would cease to exist when the pandemic is over, some other measures, such as the use of health passports, may carry on for some more time. Hence there is a need to continue to monitor the corresponding privacy risks. In this connection, DPAs would continue to play a crucial role in navigating through this 'new normal' for privacy and data protection.

51. Both Parts I and II of the Compendium have shown that, in tackling new privacy and data protection concerns arising from novel technological solutions, conventional data protection principles, such as data minimisation, purpose limitation, necessity and proportionality, transparency, etc., still provide a sound

framework for DPAs, governments and businesses in striking a balance between introducing new technological initiatives to combat the pandemic while ensuring the protection of individual privacy and personal data.

52. We hope Part II of the Compendium would be a valuable reference document for DPAs as well as for governments, health authorities and other stakeholders involved in the implementation of measures which are aimed at controlling the spread of the virus. We also hope that the Compendium will inspire DPAs and other stakeholders to come up with more good privacy practices, and encourage them to place personal data protection and privacy at the forefront of any COVID-19 response programme.

53. In short, we hope that the Compendium will serve a good reference for the protection of privacy on our road to recovery.

Office of the Privacy Commissioner for Personal Data, Hong Kong, China
October 2021

List of Resources

The following is a list of guidance or opinions published or provided by DPAs in their responses to the *Survey on Experience and Best Practices in Response to COVID-19*, in regard to data protection concerns of the COVID-19 pandemic in general, or specifically in relation to the topics of (1) Health Passport, (2) Health monitoring of incoming travellers and returning nationals, (3) Contact tracing measures, and (4) Handling of children's or students' data in e-learning technologies.

General Guidance

Source	Name of Publication / Resource	Link
IDP, Albania	Guidelines of the Office of the Commissioner on processing of personal data during telework within the measures against COVID-19	Link
	Guidelines on processing personal data in accordance with the COVID-19 Hygiene and Sanitary Protocols	Link
	Guidelines on the processing of personal data in specific sectors in the framework of measures against COVID-19	Link
	Guidelines on the protection of personal data in the context of the measures taken against COVID-19	Link
OAIC, Australia	Assessing privacy risks in changed working environments: Privacy Impact Assessments	Link
	COVID-19: Understanding privacy obligations to your staff	Link
	National COVID-19 Privacy Principles	Link
CPDP, Bulgaria	Opinion of the Commission for Personal Data Protection on the processing of personal data on the health and the level of information of employees in case of infection with COVID-19	Link
Government of Newfoundland and Labrador, Canada	Protection of Privacy Policy and Procedures Manual	Link
Data Protection Commissioner, DIFC	Force Majeure Privacy: Insights Into The Imperative For Data Protection Legislation (And FAQs)	Link

Source	Name of Publication / Resource	Link
GPDP, Italy	FAQs concerning the processing of personal data in the context of health emergency with regard to specific sectors, such as the health care sector, the workplace, schools, local authorities, clinical trials and medical research, contact tracing apps, vaccinations in the workplace (web-based information page constantly updated) [in English and Italian]	Link

Health passports

Source	Name of Publication / Resource	Link
OAIC, Australia	COVID-19 Vaccinations: understanding your privacy obligations to your staff	Link
	COVID-19 Vaccinations and my privacy rights as an employee	Link
DPAs in Canada (including OPC Canada, OIPC Newfoundland and Labrador)	Privacy and COVID-19 Vaccine Passports: Joint Statement by Federal, Provincial and Territorial Privacy Commissioners	Link
UOOU, Czech Republic	Opinion on Vaccination Passport [in Czech]	Link
	To keep customer records with some service providers and to demonstrate SARS-CoV-2 test results by customers [in Czech]	Link
	Government bill amending Act No. 258/2000 Coll., on protection public health and amending certain related laws, as amended regulations - parliamentary press 1231 - from the point of view of personal data protection [in Czech]	Link
EDPS, European Union	EDPB-EDPS Joint Opinion 04/2021 on 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) Press release	Link Link

Source	Name of Publication / Resource	Link
GPDP, Italy	Hearing of the President of the Italian DPA on constitutional aspects of the possible introduction of a "vaccination passport" for citizens who have received the anti SARS-COV2 vaccine held on 8 April 2021 [in Italian]	Link
	Warning regarding the processing of personal data carried out in relation to the Covid-19 green certificates provided for by the Legislative Decree No 52 22 of 22 April 2021 [Decision No 156 of 23 April 2021, in Italian]	Link
	Hearing of the President of the Italian DPA on issues related to the Covid-19 green certificate held on 6 May 2021 [in Italian]	Link
	'Italy reopens' decree: major criticalities for vaccination pass Italian SA issues warning to Government [press release in English]	Link
	Opinion No 229 of 9 June 2021 on the Prime Minister's draft decree concerning the implementation of the national DGC platform for the issuance of Green Pass [in Italian]	Link
	Green Pass: Green light from the Italian SA subject to adequate safeguards; Use of the IO App to be limited temporarily [press release in English]	Link
	Decision No 243 of 17 June 2021 establishing guarantees for the use of the IO App to obtain Covid-19 green certificates [in Italian]	Link
	Opinion No. 306 of 31 August 2021 on the draft decree containing amendments and additions to the implementing provisions of Article 9, paragraph 10, of the Decree-Law No 52 of 22 April 2021 [in Italian]	Link
OPC, New Zealand	Covid-19 vaccine passports not immune to privacy concerns	Link
ICO, United Kingdom	COVID-status certification: data protection expectations	Link

Health monitoring of incoming travellers and returning nationals

Source	Name of Publication / Resource	Link
DPAs in Canada (including OPC Canada, OIPC Newfoundland and Labrador)	A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19	Link
EDPS, European Union	Formal comments of the EDPS on a Proposal for a Commission Implementing Decision amending Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms	Link
GRA, Gibraltar	GDPR & DPA (20) Covid-19: Temperature Checks	Link
PCPD, Hong Kong, China	Response to media enquiry on privacy issues arising from COVID-19	Link
NPC, Philippines	NPC PHE Bulletin No. 11: Joint Statement of the Department of Health (DOH) and National Privacy Commission (NPC) on Processing and Disclosure of COVID-19 Related Data	Link
NPC, Philippines	Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response	Link

Contact tracing measures

Source	Name of Publication / Resource	Link
OAIC Australia	Guidelines for state and territory governments – Creating nationally consistent requirements to collect personal information for contact tracing purposes	Link
	Privacy obligations regarding COVIDSafe and COVID app data	Link
	The COVIDSafe app and my privacy rights	Link
OPC, Canada	Privacy review of the COVID Alert exposure notification application	Link
Government of Canada (provided by OPC, Canada)	COVID Alert: COVID-19 Exposure Notification Application Privacy Assessment	Link
DPAs in Canada	Supporting public health, building public trust:	Link

(including OPC Canada, OIPC Newfoundland and Labrador, DPA of Quebec)	Privacy principles for contact tracing and similar apps	
EDPS, European Union	TechDispatch #1/2020: Contact Tracing with Mobile Applications	Link
European Data Protection Board	Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak	Link
European Commission	Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection	Link
European Commission	COMMISSION RECOMMENDATION of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data	Link
eHealth Network, European Union	Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States	Link
eHealth Network, European Union	Interoperability guidelines for approved contact tracing mobile applications in the EU	Link
GRA, Gibraltar	GDPR & DPA (19) Covid-19: Contact Tracing and Location Data	Link
PCPD, Hong Kong, China	"LeaveHomeSafe" Mobile App in Compliance with the Requirements of the Privacy Law	Link
GPDP, Italy	Hearing through video conference of the President of the Italian Data Protection Authority regarding use of new technologies and the Internet to counter the Covid-19 epidemiological emergency held on 8 April 2020 [in English]	Link
	Opinion on the legislative proposal for the provision of an application aimed at tracing the infections from COVID-19 - April 29, 2020 [in Italian]	Link
	Authorization for the processing of personal data carried out through the Covid-19 Alert System - Immuni App - on the basis of the DPIA performed by the Ministry of Health - 1 June 2020 [in Italian]	Link
	Opinion on a draft decree of the Ministry of Economy and Finance relating to the processing of personal data carried out through the TS System as part of the Covid-19 alert system - June 1, 2020 [in Italian]	Link
	Opinion on the draft order of the Extraordinary	Link

	Commissioner for the implementation and coordination of the measures necessary for the containment and contrast of the epidemiological emergency COVID-19 - 17 December 2020 [in Italian]	
	Authorization for the processing of personal related to the COVID-19 alert system via the 'Immuni' app after the update of the data protection impact assessment carried out by the Ministry of Health, 25 February 2021[in Italian]	Link
	Opinion on a draft decree of the Ministry of Economy and Finance, in agreement with the Ministry of Health, which amends the decree of 3 June 2020, concerning the technical procedures for the involvement of the TS System for the implementation of prevention measures in the context of public health interventions related to the Covid-19 emergency - 25 February 2021 [in Italian]	Link
PPC, Japan	Personal Information Protection Commission's view on effective use of contact tracing App to help deal with Coronavirus disease (COVID-19)	Link
NPC, Philippines	NPC PHE BULLETIN No. 8: On COVID-19 - related apps, digital tools and solutions in this time of pandemic	Link
UODO, Poland	EDPB on infectious contact tracing applications [in Polish]	Link
	EDPB on applications supporting the fight against the pandemic [in Polish]	Link
	Free applications. Are they really free?	Link
FDPIC, Switzerland	Update Proximity Tracing App 30.4.2020 [in German]	Link
	Update Proximity Tracing App 13.5.2020 [in German]	Link
	Update Proximity Tracing App 12.6.2020 [in German]	Link
ICO, United Kingdom	COVID-19 Contact tracing: data protection expectations on app development	Link
	Blog: Data protection considerations and the NHS COVID-19 app	Link
	Information Commissioner's Opinion: Apple and Google joint initiative on COVID-19 contact tracing technology	Link

Handling of children's or students' data in e-learning technologies

Source	Name of Publication / Resource	Link
OPC, Canada	Education software firm addresses security vulnerabilities	Link
	International privacy guardians call for stronger protection of student privacy as e-learning expands	Link
	Investigation into CoreFour Inc.'s compliance with PIPEDA	Link
Subnational DPAs of Germany	Berlin: A Guidebook From the Data Protection Supervisory Authority for Online Learning Platforms in School Classrooms	Link
	Thuringia: Guidelines regarding data protection of e-learning platforms used by schools in Berlin	Link
PCPD Hong Kong, China	Guidelines on Children's Privacy during the Pandemic	Link
	Guidance on the Use of Video Conferencing Software	Link
	Privacy Commissioner Calls for Greater Vigilance When Teenagers Go Online; Beware of Swindlers of Personal Data	Link
GPDP, Italy	Decision of 26 March 2020 - "Distance learning: first indications" [in Italian]	Link
	Coronavirus: Information from the Italian Supervisory Authority and FAQs [in Italian and English]	Link
	Guidelines on "Integrated digital education and privacy protection": general indications" drafted by the Ministry of Education in collaboration with the Italian DPA [in Italian]	Link
	FAQs on the "PROTECTION OF PERSONAL DATA" (Section No. 11) drafted by the Ministry of Education in collaboration with the Italian DPA [Italian only]	Link
	Memorandum of the President of the Italian DPA on the "Impact of integrated digital teaching (DDI) on learning processes and on the psychophysical well-being of students"- 27 April 2021	Link
State Data Protection Inspectorate, Lithuania	Three steps for organisation of remote learning [in Lithuanian]	Link

GPDP, Macau	Suggestions on protecting the personal data of students in online learning [CN only]	Link
INAI, Mexico	Code of Good Practices to Guide the Online Processing of Personal Data of Girls, Boys and Adolescents [Spanish only]	Link
NPC, Philippines	NPC PHE BULLETIN No. 16: Privacy Dos and Don'ts for Online Learning in Public K-12 Classes	Link
	NPC PHE BULLETIN No. 17: Update on the Data Privacy Best Practices in Online Learning	Link
UODO, Poland	Security of personal data during remote learning – UODO's guide for schools	Link
	Remote work of teachers and personal data protection - advice for teachers	Link
KVKK, Turkey	Public Announcement on Distance Learning Platforms	Link
OVIC, Victoria, Australia	Collaboration Tools and Privacy	Link

Experience and Best Practices of GPA Members and Observers

Albania - Information and Data Protection Commissioner of Albania (IDP)

1. 'Health passports'[10]

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: Albanian Digital COVID Certificate
Main purpose(s): Scientific evidence of COVID-19 vaccination
Link to website:
https://e-albania.al/eAlbaniaServices/MSH/14501/MSH_14501_n4_eu_s0_web.aspx?service_code=14501

For domestic activities
Name: Digital COVID Certificate
Main purpose(s): Scientific evidence of COVID-19 VACCINATION
Link to website:
https://e-albania.al/eAlbaniaServices/MSH/14501/MSH_14501_n4_eu_s0_web.aspx?service_code=14501

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

Details (if applicable):
If you are not vaccinated you must have a tampon or pcr test. The use of the mask is necessary.

For domestic activities
Voluntary.

Details (if applicable):
The use of the mask is necessary.

[10] 'Health passports' or 'health codes' generally refer to digital solutions developed to evaluate individuals' COVID-19 infection risks by recording whether they have been vaccinated against COVID-19, received a negative test result or recovered from COVID-19, etc., often in order to facilitate cross-border/boundary travel or domestic activities. For the purpose of this survey, the use of other certificates in paper or digital form to similar effect will also be covered.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 5

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel

Personal data involved:

- Name and Surname, Fatherhood
- Age, date of birthday
- ID
- Profession of the person

Parties having access to the data:

- Family doctor
- Public Health Institution
- e-Albania is affiliated with the Government Interaction Platform
- Border police

For domestic activities

Parties having access to the data:

- Family doctor
- Public Health Institution
- e-Albania is affiliated with the Government Interaction Platform

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.
Details:
In e-Albania which is affiliated with the Government Interaction Platform.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

No.
Details: The IDP Commissioner has adopt Instruction No. 49, dated 02.03.2020 "On protection of health-related personal data". The IDP Commissioner has published 3 dedicated guidelines regarding personal data processing by the public and private controllers during the pandemic, namely:

(i) The Guidelines on the protection of personal data in the framework of antiCOVID-19 measures;
(ii) The Guidelines on personal data processing in specific sectors in the framework of anti-COVID-19 measures;
(iii) The Guidelines on personal data protection in the framework of COVID-19 Hygiene and Sanitary Measures Protocols.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

No.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

NIL.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Article 7, of law No. 9887 dated 10.03.2008 "On protection of personal data" Processing of sensitive data (Amended point 2 letter "c", "d" with law no.48/2012) provides :
1.Except for cases specified in point 2 and 3 of this Article, processing of data that reveal racial or ethnic origin, political beliefs, trade unions membership, religious or philosophical beliefs, criminal convictions and health and sexual life is prohibited. 2. Processing of sensitive data shall be done only if:
a. the data subject has given his consent, which may be revoked at any given moment making illegal any further processing of data;
b. it is in the vital interest of the data subject or another person and the data subject is physically or mentally incapable of giving his/her consent;
c. it is authorized by the responsible authority for an important public interest, under adequate safeguards;
ç. It is related to data which are manifestly made public by the data subject or is necessary for the exercise or defense of legal rights;
d. data are processed for historic, scientific or statistical research, under adequate safeguards; dh) data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care, treatment or management of health care services and data are used by medical personnel or other persons with the obligation to preserve confidentiality;
e) data are processed by non-profit political, philosophical or religious organizations and trade unions for purposes of their legitimate activity, only for members, sponsors, or other persons related to their activity. These data shall not be disclosed to a third party without the consent of the data subject unless otherwise stipulated by law. ë) data processing is necessary for the purpose of accomplishing a legal obligation and specific rights of the controller in the field of employment in compliance with the Labor Code.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

The Commissioner is in charge of:
a) giving opinions on legal and secondary draft acts related to personal data, as well as projects required to be implemented by the controller alone or jointly with others; a/1) giving recommendations for the implementation of the obligations deriving from the law on protection of personal data and assures publication thereof;
b) authorizing in special cases the use of personal data for purposes not designated during the phase of their collection by observing the principles of article 5 of this law;
c) authorizing the international transfer of personal data in compliance to article 9 herein; ç) issuing guidelines that regulate the length of retention of personal data according to their purpose in the activity of specific sectors;
d) ensuring the right to information and the exercise of the right to rectify and update data dh) authorizing the use of sensitive data in compliance with Article 7 point 2 letter 'c' herein;
e) checking the processing of data in conformity with the law, ex officio or upon request of a person when such a processing is exempted of the right to information and to inform the person that the check is carried out and whether the process is lawful or not; ë) addressing of complaints the data subject related to the protection of his/her rights and freedoms, for processing of personal data and informing him/her on the

settlement of the complaint submitted;
f) issuing guidelines on security measures in the activity of specific sectors,
g) overseeing the execution of penalties; gj) encourage the controller to draft the of codes of ethics and their assessment;
h) the publication and explanation of the rights related to the data protection and the periodic publication of his activities;
i) cooperating with the supervisory authorities on the personal data of foreign states regarding the protection of individuals who reside in those states;
j) representing the supervisory authority in the field of personal data protection in the national and international events;
k) exercising other legal obligations.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

- Guidelines of the Office of the Commissioner on processing of personal data during telework within the measures against COVID-19;
- Guidelines on processing personal data in accordance with the COVID-19 Hygiene and Sanitary Protocols;
- Guidelines on the processing of personal data in specific sectors in the framework of measures against COVID-19
- Guidelines on the protection of personal data in the context of the measures taken against COVID-19

***

https://www.idp.al/2021/03/02/guideline-of-the-office-of-the-commissioner-on-processing-of-personal-data-during-telework-within-the-measures-against-covid-19/?lang=en
https://www.idp.al/2020/05/06/guidelines-for-processing-personal-data-in-accordance-with-the-covid-19-hygiene-and-sanitary-protocols/?lang=en
https://www.idp.al/2020/04/06/guideline-on-the-processing-of-personal-data-in-specific-sectors-in-the-framework-of-measures-against-covid-19/?lang=en
https://www.idp.al/2020/03/20/guidelines-on-the-protection-of-personal-data-in-the-context-of-the-measures-taken-against-covid-19/?lang=en

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

NIL.

2. Health monitoring of incoming travellers and returning nationals

Not applicable.

3. Contact tracing measures

Not applicable.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Microsoft 365 (Teams), Zoom, Webex.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Yes. This is a requirement set out in Instruction 47 of the Commissioner.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

The information of data subjects related to their rights regarding the processing of personal data using these e-learning platforms.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

The principles applied by Article 5 of the current data protection legislation in Albania are the same as those applied in the Directive 95/46.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes, we have issued guidelines and bylaws related, among others, to the education sector.

4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.

Yes, in addition to the issued guidelines and bylaws, we have exercised our authority regarding administrative inspections in Health Institutions (both Public & Private), as well as in the Education Sector (mostly Universities).

Bulgaria - Commission for Personal Data Protection (CPDP)

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

1. ‘Health passports’
1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?
For cross-border/boundary travel Yes. *For domestic activities* No.
1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).
For cross-border/boundary travel Name: Digital Green Certificate Main purpose(s): The EU Digital COVID Certificate should facilitate free movement inside the EU Description: Link to website: https://www.his.bg/
1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.
For cross-border/boundary travel Voluntary.
1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?
Rating (on a scale of 1 – 5): 3
1.5 Please list out the personal data involved in the ‘health passport’ or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.
For cross-border/boundary travel Personal data involved: • Vaccination status; • COVID-19 test results Parties having access to the data: • Health authorities

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details: The Ministry of Health stored or processed the data in the central database

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

No.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

People who have a Green certificate travel within the EU without having to present a negative Covid-19 test, they are not subject to mandatory quarantine and travel freely and without giving a good reason.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

The principles set out in Article 5 of the GDPR are respected

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

Consultation/Advisory.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

- Opinion of the Commission for Personal Data Protection on the processing of personal data on the health and the level of information of employees in case of infection with COVID-19
- The Bulgarian SA participates in the preparation and implementation of EDPB-EDPS Joint Opinion 04/2021 on 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)

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

NIL.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Certificate of completed vaccination;
- A document showing a positive PCR result or a rapid COVID-19 antigen test for individuals who have recovered from COVID-19 between 15 and 180 days from the date of the positive test result;
- Document showing a negative result from a COVID-19 test - PCR test performed within 72 hours before entry into the country or
- Document showing a negative result from a COVID-19 test - antigen test performed within 48 hours before entry into the country)

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Processing special categories data.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

The principles set out in Article 5 of the GDPR are respected.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Consultation/ Advisory.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The Bulgarian SA provides advice to health authorities, Ministry of Transport, and participates in the preparation and implementation of EDPB-EDPS Joint Opinion 04/2021 on 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).

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Opinion of the Commission for Personal Data Protection on the processing of personal data on the health and the level of information of employees in case of infection with COVID-19

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.
What best describes the approach used to build the contact tracing app?
Centralised approach.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Virusafe
Description: The purpose of this application is to enable all residents in the Republic of Bulgaria to get involved and help, enter data and report their condition every day.
Link to website: https://app.coronavirus.bg/

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.
Link to relevant legislation:
Act on the Measures and Actions During the State of Emergency Declared with the Decision of the National Assembly of March 13th, 2020

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

The principles set out in Article 5 of the GDPR are respected and Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Consultation/ Advisory.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The Bulgarian CPD provides advice to health authorities and mobile application developers, but is mainly guided by Guidelines 04/2020 on the use of location data and contact tracking tools in the context of the COVID-19 outbreak.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks

associated with the development and use of the contact tracing app? Please provide real examples if possible.
NIL.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?
Yes, significant increase.
4.2 What are the popular e-learning technologies used in your jurisdiction?
Microsoft Teams; Shkolo (https://www.shkolo.bg/)
4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?
Yes.
4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?
High risk to the rights and freedoms of the persons.
4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?
The principles set out in Article 5 of the GDPR are respected.
4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
Individual consultations and direct answer to the specific questionary.
4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.
NIL.

Canada - Office of the Privacy Commissioner of Canada (OPC)

Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner of Canada

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Not yet, but it is being planned / considered by the government.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: Arrive Can
Main purpose(s): allow border authorities to confirm vaccination status of travellers

For domestic activities
Name: TBD
Main purpose(s): allow border authorities to confirm vaccination status of travellers

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Mandatory and voluntary.

Details (if applicable): While not a constituting a specialized health passport (or replacing the role of a traditional government-issued passport), the Arrive Can application (a customs-declaration tool) will allow travellers to upload proof of vaccination next month allowing travellers an exemption from quarantine. It is not mandatory (in the sense that you can choose to upload vaccine information to obtain an exemption) but providing some vaccination status information at the border is necessary.

For domestic activities
Voluntary.

Details (if applicable): while not constituting a passport per se the Governments of Quebec and Ontario have begun to issue digital vaccination proofs with machine-readable QR codes.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): according to recent polling between 3 to 4 depending upon the particular context of their use.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

TBD

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details: With Arrive CAN, proof of vaccine information will be centrally stored with the Canadian border authority.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

Major privacy risks: OPC has not yet received PIA but it is underway and will review the privacy assessment post deployment; however PHAC/CBSA has consulted our Office throughout the development. (PIA work in advance was something privacy commissioners across Canada have recommended)

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

TBD (Effectiveness assessment is something privacy commissioners across Canada have recommended)

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

TBD (Independent oversight is something that privacy commissioners across Canada have recommended)

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

TBD

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

In May Privacy commissioners at the federal and provincial levels across Canada recommended a series of key principles including:

- Clear legal authority
- Consent
- Limits on collection use and disclosure
- Transparency
- Accountability
- Safeguards
- Independent oversight
- Time and scope limitations

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

Advice through consultations and or review of privacy impact assessment.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210519/ and https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

TBD

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.
Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Transparency and Necessity: Both verbal and written notice statements must clearly describe all collections, uses and disclosures of personal information and should be proactively provided at all points of contact. Particularly as it relates to onward disclosures of personal information collected at the border, authorities should clearly communicate with travellers and limit disclosures to only that which is necessary to monitor compliance with the law. The basis of questions posed to travellers should be explained to demonstrate their necessity and the connection to the purpose of the program.

Purpose Limitation, oversight and accountability: Clear oversight mechanisms must be well documented. Furthermore, responsible parties should develop a robust oversight mechanisms to ensure that it is accountable for decision-making processes related to compliance activities.

Time Limitation: It is unclear for how long it may be necessary to monitor the health of incoming travellers in relation to COVID-19 however, efforts should made to prioritize identifying an appropriate set of parameters. Furthermore, retention periods for information collected in relation to COVID-19 must be put in place.

Vulnerable Populations: The impacts on vulnerable populations should be assessed, particularly as they relate to quarantine measures.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

The OPC outlined key privacy and data protection principles for pandemic-response in guidance to government posted in April 2020.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Guidance and advice through consultation.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Main privacy and data protection principles for pandemic-response in OPC guidance to government included legal authority, assessment of necessity and proportionality, purpose limitation, safeguards, attention to effects on vulnerable populations, transparency, accountability, and time limitation.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

- Conducing a privacy assessment
- Secure application
- The use of privacy notice statements
- Defined legal authority

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: COVID Alert app
Description: The app uses Bluetooth to exchange random codes between your phone and nearby phones. Each day, the app checks a list of random codes from users who have informed the app, through a one-time key, they've tested positive for COVID-19.
Link to website: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks: handling of one-time keys and IP addresses were given significant analysis in the government assessment as well as questions of consent as well as necessity and proportionality

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

The OPC review of the government's assessment also emphasized issues of proportionality and consent and accountability as well as robust safeguards

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Review of the program privacy assessment in addition to participation in effectiveness audit of program.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Joint statement issued by federal, provincial and territorial Privacy Commissioners (May 2020) Supporting public health, building public trust: Privacy principles for contact tracing and similar apps stressed consent and purpose limitation and time limitation. Transparency accountability and safeguards were also emphasized.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.
Please refer to Note 2 in the Annex

- Conducting a privacy assessment
- Secure application
- Limited collection of personal information
- Decentralised model of data storage

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Google Classroom.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

In Canada education is a provincial and municipal responsibility which means our authority does not have direct jurisdiction over educational institutions or handling of student data.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Our office's recent investigation into an education software company identified certain security safeguard vulnerabilities and the lack of a privacy management framework commensurate with the volume and sensitivity of the PI involved.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Our recent investigation into an education software firm emphasized the importance of safeguards and accountability.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The GPA resolution on e-learning platforms from 2018. We recently published the results of an investigation into an education software firm with certain security vulnerabilities that highlights the importance of implementing safeguard enhancements and having a privacy management framework.

4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.

Not applicable.

Croatia - Croatian Personal Data Protection Agency (AZOP)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: EU Digital COVID Certificate
Main purpose(s): facilitating cross-border travelers during COVID-19 pandemic
Description: Legal basis for EU Digital COVID Certificate is 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 (EU digital COVID certificate)
Link to website: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130

For domestic activities-
Name: EU Digital COVID Certificate
Main purpose(s): preventing the spread of SARS-CoV-2
Description: the security measures prescribed by national law may be ordered by decision of Civil Protection Headquarters of the Republic of Croatia, in cooperation with the Ministry of Health and the Croatian Institute of Public Health.
Link to website: https://civilna-zastita.gov.hr/odluke-stozera-civilne-zastite-rh-za-sprecavanje-sirenja-zaraze-koronavirusom/2304

1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Mandatory.

Details (if applicable): Usage of EU Digital COVID Certificate is mandatory by 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 (EU digital COVID certificate)

For domestic activities
Mandatory.

Details (if applicable): The security measures prescribed by national law may be ordered by decision of Civil Protection Headquarters of the Republic of Croatia, in cooperation with the Ministry of Health and the Croatian Institute of Public Health. The decisions ordered by Civil Protection Headquarters of the Republic of Croatia are mandatory.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 3

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: Please see the Annex of the above-mentioned regulation which defines certificate datasets which are included in the certificate.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130
Parties having access to the data: Authorized persons in the competent authorities.

For domestic activities
Personal data involved: Please see the Annex of the above-mentioned regulation which defines certificate datasets which are included in the certificate.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130
Parties having access to the data: Authorized persons in the competent authorities.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

Details: Regulation prohibits retention of personal data obtained from the certificate by the Member State of destination or transit or by the cross-border passenger transport services operators.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks: It is inappropriate to share our views since we do not have all information needed to answer this question.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.

Details: It is inappropriate to share our views since we do not have all information needed to answer this question.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.

Details: Regulation implements certain public health measures only during the COVID-19 pandemic.
The Act on the Protection of the Population from Infectious Diseases is in force, Article 47 sets out security measures to protect the population from infectious diseases, including for example the prohibition/restriction of public and private gatherings.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

It is inappropriate to share our views since we do not have all information needed to answer this question.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

It is inappropriate to share our views since we do not have all information needed to answer this question.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

Our role is of an advisory/supervisory nature in accordance with the powers/tasks given by the General Data Protection Regulation and national Law on the Implementation of the General Data Protection Regulation.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

We have given advice regarding the obligations prescribed by the GDPR.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

It is inappropriate to share our views since we do not have all information needed to answer this question.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.
Relevant requirements
Testing for COVID-19.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

In our experience, the weak point is the insufficiently implemented technical and organizational measures.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

To our opinion the key principles are data minimization, integrity and confidentiality, storage limitation.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

It is inappropriate to share our views since we do not have all information needed to answer this question.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

It is inappropriate to share our views since we do not have all information needed to answer this question.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Stop COVID-19
Description: Stop COVID-19 is an application that serves to simply warn citizens that they may have found themselves in epidemiologically risky contact. It will help you make the right decision if you develop symptoms: you will be able to give the epidemiologist accurate and clear information about the exposure. If you have no symptoms, and the application warns you that you have been in epidemiologically risky contact, you can pay more attention to hygiene and physical distance.
Link to website: https://www.koronavirus.hr/stop-covid-19-723/723

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

We do not have information on the above mentioned.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

To our opinion the key principles are data minimization, integrity and confidentiality, storage limitation.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

None.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes, we advised stakeholders that personal data should not be processed via contact tracing app.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Not applicable.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Distance communication platforms for the purpose of conducting online teaching.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Yes.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

The concerns are related to Chapter V of the GDPR and the possible non-transparency of the processing of personal data of vulnerable groups such as children.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

To our opinion the key principles are lawfulness, fairness and transparency.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.
We were conducting online workshops for educational sector in order to mitigate privacy risks by sharing knowledge to raise awareness of personal data protection during COVID-19 pandemic time.

Czech Republic - Office for Personal Data Protection (UOOU)

1. ‘Health passports’
1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?
For cross-border/boundary travel Yes. *For domestic activities* Yes.
1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).
For cross-border/boundary travel Name: **Tečka** and **čTečka** Main purpose(s): The application Tečka allows parties upload and save certificates from https://ocko.uzis.cz and present them to enable border crossing, access to services or at an event. The application čTečka allows verification of information provided by Tečka. Link to website: https://ockodoc.mzcr.cz/napoveda/tecka/cz/ *For domestic activities* Name: Tečka Main purpose(s): The application allows upload and save certificates from https://ocko.uzis.cz and present them to enable border crossing, access to services or at an event. Link to website: https://ockodoc.mzcr.cz/napoveda/tecka/cz/
1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.
For cross-border/boundary travel Voluntary. *For domestic activities* Voluntary.
1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?
Rating (on a scale of 1 – 5): 4

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: Name, surname, date of birth, as well as information on whether the person has been vaccinated, has suffered from COVID-19 or has a negative AG or PCR test result, where a unique identifier is assigned.
Parties having access to the data: Various subjects of public administration and the private sector.

For domestic activities
Personal data involved: Name, surname, date of birth, as well as information on whether the person has been vaccinated, has suffered from COVID-19 or has a negative AG or PCR test result, where a unique identifier is assigned.
Parties having access to the data: Various subjects of public administration and the private sector.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details: Both Tečka and čTečka read from centralized database, but there is no DPIA for it. Some information may be found at https://ockodoc.mzcr.cz/napoveda/tecka/cz/podminky-pouzivani/ and https://ockodoc.mzcr.cz/napoveda/tecka/cz/.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

Major privacy risks: The Czech DPA has no information about DPIA for both Tečka and čTečka. The Czech DPA was not sufficiently consulted.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

No.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

No.

Details: Due to the new types of termination mutations, there is currently no type of debate.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

NIL.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

In general, personal data and their processing should be used to empower individuals rather than control them. As the processing includes (but is not limited to) health data, it is a processing of a special category of data under Article 9 of the GDPR and thus requires a high level of security and an emphasis on data minimization.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

It must be said that consultations with the supervisory authority were not sufficient.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes, Czech DPA has issued several opinions:
https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=50807
https://www.uoou.cz/k-vedeni-evidence-zakazniku-nekterymi-poskytovateli-sluzeb-a-k-prokazovani-vysledku-testu-na-sars-cov-2-ze-strany-zakazniku/d-49643

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

There has been a strong call by the Czech DPA that the use of a digital green certificate should not lead to direct or indirect discrimination against individuals and should be fully in line with the principles of necessity, effectiveness and proportionality:

https://www.uoou.cz/uoou-k-tzv-ockovacim-pasum/d-49208

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

In the case of the government, it is primarily a requirement of legality that requires consideration
the processing of personal data has been described to the maximum of its parameters. It is not meant only
a list of processed personal data, only minimal and necessary, but also accurate
the definition of the objective pursued by the proposed procedure, including the purposes for which it may be personal data collected and used.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Minimization and efficiency.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Very limited due to insufficient cooperation with the Ministry of Health.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Not yet.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

NIL.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: eRouška
Description: The application eRouška 2.1 detects and stores the identifiers of other telephones with eRouška in the vicinity via BLE technology. When someone gets sick, he or she may easily warn others about the possible risk of infection via the application.
Link to website: https://erouska.cz/

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, existing legislation was amended.

Link to relevant legislation: https://www.zakonyprolidi.cz/cs/2021-94

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
From the point of view of Czech DPIA, the DPIA was not sufficient.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Minimization and efficiency.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Very limited due to insufficient cooperation with the Ministry of Health.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Strong warning that the original eRouška 1.0, based on centralized BlueTrace protocol, processed personal data despite the declaration that it would use anonymized data only.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

The eRouška 2.1 application is based on voluntariness. No one can be forced to use it.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Teams, Zoom & Google.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

NIL.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?
Communication between participants is not end-to-end encrypted (Zoom said in marketing materials that it was, but in the end he was forced to apologize for this statement). End encryption only appears for text chat, video and audio are not protected, encryption is used only for transmission.
4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?
Do not send many details about the phone, advertising ID or location.
4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
NIL.
4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.
NIL.

Dubai International Financial Center (DIFC) – Data Protection Commissioner

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Not yet, but it is being planned / considered by the government.

For domestic activities
Not yet, but it is being planned / considered by the government.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

Currently not applicable but the initial stages of being allowed to travel internationally or attend domestic events requires showing of the national and / or emirate level Covid tracking and vaccination recording app, or of a negative PCR test. Emirates airlines requires an additional undertaking form to be completed. So the elements are starting to take shape.

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Mandatory.
To the extent that the above can be considered the foundations of such health passport in the UAE.

For domestic activities
Mandatory.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 4

The public generally are willing to accept resources and applications that help all of us get healthy and being undertaking "normal" activities again, including sharing personal data for this purpose. They are however a bit wary about uses for other purposes, as presumably most data subjects anywhere might be when sharing personal data with a government entity. Most of the general public are EU, UK, US or Australia / NZ ex pats though, so they have a very keen understanding or awareness of DP issues and concerns, and are savvy to personal data processing activities and rights.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

As above.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.
No information on this yet – probably will be centrally stored.
1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?
DIFC have done their own DPIA. Risks are as you may imagine: • Data breaches with respect to highly sensitive personal data • Misuse of personal data for other purposes not previously notified to data subjects • Prohibitions on personal freedoms and undue influence of the authorities if not vaccinated or PCR tested
1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
Not applicable at this time but there likely will be regular reviews, yes.
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
No info available at this time.
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
Please see Articles 26 and 27 of DIFC DP Law – includes MOUs with other government agencies to assure Article 28 rights. https://www.difc.ae/application/files/6115/9358/6486/Data_Protection_Law_DIFC_Law_No.5_of_2020.pdf/
1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?
They will likely be national security / substantial public interest based, but in general they are the common principles shared by all mature DP Laws. Please see Article 9 of the DIFC DP Law for guidance, although again this is not currently confirmed to be the position of the UAE government.
1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?
DIFC Commissioner's Office may be asked to consult in development of such measures.
1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
DIFC have developed Covid 19 guidance, yes, and we are updating our guidance accordingly. The current guidance is: https://dg23rp0isu1uj.cloudfront.net/application/files/2016/1241/5829/Covid_19_FAQs

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

To be determined, and updated in guidance to share with UAE government upon request.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine (if necessary)
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Please see response to 1.7 above.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Please see response to 1.11 above.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

No involvement at this time. This sits with a Dubai and UAE government health ministry.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Please see response to 1.13 above.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Please see response to 1.14 above.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes, in theory. Cannot respond to further questions at this time.

4. Handling of children's or students' data in e-learning technologies

DIFC does not have schools, etc., in its jurisdiction as we are a financial center.

Estonia - Estonian Data Protection Inspectorate

REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

1. 'Health passports'[11]

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Not yet, but it is being planned / considered by the government.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: EU Digital COVID Certificate (includes COVID Vaccination, Testing and Recovery certificates)
Main purpose(s):
Travelling (Certification itself is not a ground for entry to the country, it may be a ground for exemption from restrictions, such as self-isolation, in the country of destination. When traveling the possible restrictions in the country of destination should be taken into account).
Description:
A person can print or download the certificate (with QR code) from Estonian e-Health system. The certificate with a QR code is generated in case of vaccination, negative test result or recovery from the disease.

Link to website: www.digilugu.ee, more information: https://www.kriis.ee/et/vaktsineerimistoend

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

Details (if applicable):
The certificate is not a basis for travel abroad, but may be exempted from restrictions imposed by the country (e.g. self-isolation) depending on the requirements of the country of destination. When traveling, the requirements of the country of destination must be taken into account when entering / imposing isolation obligations.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 5

[11] The information contained in this section was collected in July 2021, and there have been changes regarding the health passports in Estonia since then.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel

Personal data involved: First and last name and date of birth.

- Vaccination certificate: In addition to personal data, it has a certificate number; the disease against which it was vaccinated; active ingredient; immune preparation; the marketing authorization holder of the vaccine; number in a series of vaccinations; date of immunization and country of immunization. Also the details of the issuer of the certificate.
- Test certificate: In addition to personal data, it has a certificate number; the disease being tested; type of analysis; time of sampling; the result of the analysis; the authority that performed the analysis and the country where the test was performed. There is also the data of the issuer of the certificate.
- Recovery certificate: In addition to personal data, it has a certificate number; the disease being tested; the date of the first positive test; country where tested; the periods of validity of the certificate. Also the details of the issuer of the certificate.

Parties having access to the data: The health information for creating the certificate is located in the Estonian e-Health System. The access to the system is limited and listed in the relevant legislation. For example a doctor can have access to the patient's information only in case of treatment. Using a certificate does not mean that the other party has an access to the e-Health System. The certificate just allows to prove the veracity of the information transmitted by the health care professional to the e-Health System.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.
DPIA was conducted during the process of amendment of the law and it was presented in the draft amendment of the law.
Major privacy risks: not able to provide

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Not able to provide information.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Not able to provide information.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

Estonian certificates are based on the uniform EU Digital COVID Certificate.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Must have legal bases, purposes, security measures.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

Providing advice, giving opinion to the draft law amendments.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

Must fulfil the requirements coming from the GDPR, such as: transparency requirements, minimisation of personal data, use and disclosure limitation, data security measures.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Testing for COVID-19
  - A test is required for entry from third countries that are not on the so-called green list of the European Union and who have not undergone a vaccination course. Citizens, permanent residents and citizens of the European Union are not required to take the test.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Not able to provide information.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Not able to provide information.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Providing consultation when necessary.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Not able to provide information.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Estonian schools have official/obligatory digital environments (such as eKool https://www.ekool.eu/#/about, Stuudium https://stuudium.com/) to connect pupils (and their parents) and schools, providing diary, study material management, in-depth communication module etc. Beside these the online lessons were usually provided through MS Teams, Zoom and other similar platforms.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

DPIA has to be conducted when obligatory (foreseen in the GDPR) and the Inspectorate requires it when necessary (during consultations, enforcement procedures etc.)

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Security risks (data collection, storage, deletion, transfer etc), recording of audio and video of lessons

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Legal base and purposes, data security, transparency

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
We haven't issued guidance, but we have informed schools and other institutions about the (data protection) requirements. Also, we have provided consultations on these subjects.
4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.
Must fulfil data protection regulation (the GDPR), such as the necessity, effectiveness and proportionality, appropriate data security measures, adequate safeguards for cross-border transfer of personal data collected.

European Union - European Data Protection Supervisor (EDPS)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

The EU has launched and approved a Regulation providing for the creation of an EU Digital COVID Certificate.

The EU Digital COVID Certificate will facilitate safe free movement of citizens in the EU during the COVID-19 pandemic. The certificate will be introduced in EU Member States. Countries can start issuing and using it already and it will become available in all EU Member States as of 1 July 2021.

An EU Digital COVID Certificate is a digital proof that a person has either

- been vaccinated against COVID-19
- received a negative test result or
- recovered from COVID-19

The certificate will be:

- Digital and/or paper format
- with QR code
- free of charge
- in national language and English
- valid in all EU countries

National authorities are in charge of issuing the certificate. It could, for example, be issued by test centres or health authorities, or directly via an eHealth portal. The digital version can be stored on a mobile device. Citizens can also request a paper version. Both will have a QR code that contains essential information, as well as a digital signature to make sure the certificate is authentic. Member States have agreed on a common design that can be used for the electronic and paper versions to facilitate the recognition.

How will the certificate work?

- The EU Digital COVID Certificate contains a QR code with a digital signature to protect it against falsification.
- When the certificate is checked, the QR code is scanned and the signature verified.
- Each issuing body (e.g. a hospital, a test centre, a health authority) has its own digital signature key. All of these are stored in a secure database in each country.

The European Commission has built a gateway through which all certificate signatures can be verified across the EU. The personal data of the certificate holder does not pass through the gateway, as this is not necessary to verify the digital signature. The European Commission also helped Member States to develop national software and apps to issue, store and verify certificates and supported them in the necessary tests to on-board the gateway.

The EU Digital COVID Certificate contains necessary key information such as name, date of birth, date of issuance, relevant information about vaccine/ test/recovery and a unique identifier. This data remains on the certificate and is not stored or retained when a certificate is verified in another Member State.
The certificates will only include a limited set of information that is necessary. This cannot be retained by visited countries. For verification purposes, only the validity and authenticity of the certificate is checked by verifying who issued and signed it. All health data remains with the Member State that issued an EU Digital COVID Certificate.

For cross-border/boundary travel
No.
At present the EU Digital COVID Certificate is only valid within the EU territory.

The Regulation only provides for the Certificate to be used for the purpose of freedom of movement within EU Member States. Should the European Member States reuse the Certificate for national purposes, this and the personal data related to it at Member States level must respect Articles 7 and 8 of the EU Charter of Fundamental Rights and must be in compliance with the GDPR, including Article 6(4) GDPR15. This implies the need for a proper legal basis in Member State law, complying with the principles of effectiveness, necessity, proportionality and including strong and specific safeguards implemented following a proper impact assessment, in particular to avoid any risk of discrimination16 and to prohibit any retention of data in the context of the verification process.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For EU travel:

Name: EU Digital COVID Certificate
Main purpose(s): facilitate the freedom of movement within the EU Member States
Description: see above for the description.
Link to website: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_env; https://eur-lex.europa.eu/eli/reg/2021/953/oj

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For EU travel

The Regulation approved requires all EU Member States to use the EU Digital COVID Certificate framework and issue certificates for the purpose of facilitating the exercise of the right to free movement within the EU during the COVID-19 pandemic.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): The EDPS does not have the data to provide an acceptance rate.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

Data fields to be included in the vaccination certificate:

(a) name: surname(s) and forename(s), in that order;
(b) date of birth;
(c) disease or agent targeted: COVID-19 (SARS-CoV-2 or one of its variants);
(d) COVID-19 vaccine or prophylaxis;
(e) COVID-19 vaccine product name;
(f) COVID-19 vaccine marketing authorisation holder or manufacturer;
(g) number in a series of doses as well as the overall number of doses in the series;
(h) date of vaccination, indicating the date of the latest dose received;
(i) Member State or third country in which the vaccine was administered;
(j) certificate issuer;
(k) unique certificate identifier.

2. Data fields to be included in the test certificate:

(a) name: surname(s) and forename(s), in that order;
(b) date of birth;
(c) disease or agent targeted: COVID-19 (SARS-CoV-2 or one of its variants);
(d) the type of test;
(e) test name (optional for NAAT test);
(f) test manufacturer (optional for NAAT test);
(g) date and time of the test sample collection;
(h) result of the test;
(i) testing centre or facility (optional for rapid antigen test);
(j) Member State or third country in which the test was carried out;
(k) certificate issuer;
(l) unique certificate identifier.

3. Data fields to be included in the certificate of recovery:

(a) name: surname(s) and forename(s), in that order;
(b) date of birth;
(c) disease or agent from which the holder has recovered: COVID-19 (SARS-CoV-2 or one of its variants);
(d) date of the holder's first positive NAAT test result;
(e) Member State or third country in which test was carried out;
(f) certificate issuer;
(g) certificate valid from;
(h) certificate valid until (not more than 180 days after the date of first positive NAAT test result);
(i) unique certificate identifier.

The parties who may have access to the data will be decided by national Member States.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

Details: In accordance with recital 52 of the Regulation, it *"(...) does not provide a legal basis for setting up or maintaining a centralised database at Union level containing personal data."*

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

The European Commission has not done any Privacy Impact Assessment. This has been criticised by the European Data Protection Board (EDPB) and the EDPS in their Joint Opinion on the Proposal (at the time), in para. 16 of the Joint Opinion: "*(...) the EDPB and the EDPS underline the lack of an impact assessment accompanying the Proposal, that would provide substantiation as to the impact of the measures being adopted as well as to the effectiveness of already existing less intrusive measures."*

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.

Details:
Article 16 of the Regulation states that:

1. By 31 October 2021, the Commission shall submit a report to the European Parliament and to the Council. The report shall include an overview of: (a) the number of certificates issued pursuant to this Regulation; (b) guidance requested pursuant to Article 3(11) on the available scientific evidence and level of standardisation regarding the possible issuance of certificates of recovery based on antibody tests, including serological testing for antibodies against SARS-CoV-2, taking into account the availability and accessibility of such tests; and (c) the information received pursuant to Article 11.

2. By 31 March 2022, the Commission shall submit a report to the European Parliament and to the Council on the application of this Regulation. The report shall contain, in particular, an assessment of the impact of this Regulation on the facilitation of free movement, including on travel and tourism and the acceptance of the different types of vaccine, fundamental rights and non-discrimination, as well as on the protection of personal data during the COVID-19 pandemic.

The report may be accompanied by legislative proposals, in particular to extend the period of application of this Regulation, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.

Details:
Article 17 of the Regulation clearly states that:

This Regulation shall enter into force on the day of its publication in the Official Journal of the European Union. It shall apply from 1 July 2021 to 30 June 2022.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

No international transfers of personal data to third countries are envisaged in the Regulation.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Article 10 of the Regulation provides for the data protection principles to apply:

1. Regulation (EU) 2016/679 shall apply to the processing of personal data carried out when implementing this Regulation.
2. For the purpose of this Regulation, the personal data contained in the certificates issued pursuant to this Regulation **shall be processed only for the purpose of accessing and verifying the information included in the certificate in order to facilitate the exercise of the right of free movement within the Union during the COVID-19 pandemic**. **After the end of period of the application of this Regulation, no further processing shall occur**.
3. The personal data included in the certificates referred to in Article 3(1) shall be processed by the competent authorities of the Member State of destination or transit, or by the cross-border passenger transport services operators required by national law to implement certain public health measures during the COVID-19 pandemic, only to verify and confirm the holder's vaccination, test result or recovery. To that end, the personal data shall be limited to what is strictly necessary. The personal data accessed pursuant to this paragraph shall not be retained.
4. The personal data processed for the purpose of issuing the certificates referred to in Article 3(1), including the issuance of a new certificate, shall not be retained by the issuer longer than is strictly necessary for its purpose and in no case longer than the period for which the certificates may be used to exercise the right to free movement.
5. Any certificate revocation lists exchanged between Member States pursuant to Article 4(2) **shall not be retained after the end of period of the application of this Regulation**.
6. The authorities or other designated bodies responsible for issuing the certificates referred to in Article 3(1) shall be considered to be controllers as defined in point (7) of Article 4 of Regulation (EU) 2016/679.
7. The natural or legal person, public authority, agency or other body that has administered a COVID-19 vaccine or carried out the test for which a certificate is to be issued shall transmit to the authorities or other designated bodies responsible for issuing the certificates the personal data necessary to complete the data fields set out in the Annex. 8. Where a controller as referred to in paragraph 6 uses a processor for the purposes referred to in Article 28(3) of Regulation (EU) 2016/679, no transfer of personal data by the processor to a third country shall take place.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

The EDPB and the EDPS have been consulted by the European Commission to issue a Joint Opinion on the Proposal (at the time).

The EDPB-EDPS Joint Opinion 04/2021 on 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) can be found here: https://edps.europa.eu/system/files/2021-04/21-03-31_edpb_edps_joint_opinion_digital_green_certificate_dcg_en.pdf.

In the current emergency situation caused by the COVID-19 pandemic, the EDPB and the EDPS have insisted that the principles of effectiveness, necessity, proportionality and non-discrimination are upheld. The EDPB and the EDPS have reiterated that, at the moment of writing of the Opinion, there seemed to be little scientific evidence as to whether having received the COVID-19 vaccine (or having recovered from COVID-19) grants immunity, and, by extension, how long such immunity may last, but that scientific evidence is growing daily.

Moreover, a number of factors are still unknown regarding the efficacy of the vaccination in reducing transmission. The Proposal should lay down clear and precise rules governing the scope and application of

the Digital Green Certificate and impose appropriate safeguards. This will allow individuals, whose personal data is affected, to have sufficient guarantees that they will be protected, in an effective way, against the risk of potential discrimination.

The EDPB and the EDPS have stated that the Proposal must expressly include that access to and subsequent use of individuals' data by EU Member States once the pandemic has ended is not permitted. At the same time, the EDPB and the EDPS have highlighted that the application of the proposed Regulation must be strictly limited to the current COVID-19 crisis.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

See answer to question 1.12: EDPB-EDPS Joint Opinion 04/2021 on 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)

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

- Transparency requirements in the development and use of health passports or similar measure(s)
- Minimisation of the collection and retention of personal data
- Use and disclosure limitation, preventing misuse for further incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Ethical concerns, such as the risk to discrimination and the right to liberty of movement
- Efficacy and effectiveness of the 'health passports' or similar measure(s)

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

In the context of the COVID19 emergency, the European Commission has taken and is taking all necessary steps to coordinate with Member States and to facilitate the supply of protective and medical equipment across Europe: (https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/public-health_en).

The handling of health data is a competence of EU Member States.

The national Member States will decide on the requirements and measures to monitor the health of incoming travellers and returning nationals. However, from 1st of July (entry into force of the EU Digital COVID Certificate Regulation), the Member States will be able to issue and accept the Certificate and possibly waive certain restrictions.

In addition, a Commission Implementing Decision (EU) 2021/858 of 27 May 2021 amending

Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms has entered into force, and aims to ensure interoperability between national Member States performing contact tracing at national level.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

The national Member States will decide on the requirements and measures to monitor the health of incoming travellers and returning nationals. The privacy risks are high, particularly due to the reason that sensitive data such as health data is being processed in this regard.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

- Defining a clear legal basis for the processing of personal data;
- Data minimisation;
- Limiting the disclosure/ access to personal data;
- Clear purpose limitation;
- Setting strict data retention periods;
- Ensuring the security of data;
- Ensuring the accuracy of the data;
- Involving data protection authorities.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

As the data protection supervisor for EUIs, the EDPS has not been involved in national measures' implementation.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The EDPS has been formally consulted by the European Commission on the Passenger Locator Form Implementing Decision: https://edps.europa.eu/system/files/2021-05/201-0445_d0956_comments_en.pdf

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

NIL.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No.

The EU as such has not adopted any digital contact tracing or a location tracking measure aimed at containing the spread of COVID-19 as such.

However, it has developed multiple guidance in relation to contact tracing and location tracking, in particular:

- The European Commission has issued a Recommendation, dated 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data;
- The eHealth Network, a voluntary network set up under article 14 of Directive 2011/24/EU, and providing a platform of Member States' competent authorities dealing with digital health, has published a common toolbox on the use of mobile applications to support contact tracing in the EU's fight against COVID-19. It has also published its interoperability guidelines for approved contact tracing mobile applications in the EU.
- The Commission has also provided Guidance on Apps supporting the fight against Covid19 pandemic in relation to data protection.

The main recommendations and principles that have been made for an accountable use of contact tracing applications include:

- Ensuring that national health authorities (or entities carrying out tasks in the public interest in the field of health) are the data controllers of the personal data;
- Ensuring that the individual remains in control, by underlining the **voluntary use of the application**, without any negative consequences for the individual who decides not to download/use the app. In terms of technology, the **Bluetooth Low Energy (BLE) technology** was considered the best approach as the communications between devices appears more precise, and therefore more appropriate, than for example the use of geolocation data (GNSS/GPS, or cellular location data), which would likely not work indoor, sometimes even outdoor, due to the limited precision;
- Defining a clear legal basis for the processing of personal data;
- Data minimisation;
- Limiting the disclosure/ access to personal data;
- Clear purpose limitation;
- Setting strict data retention periods;
- Ensuring the security of data;
- Ensuring the accuracy of the data;
- Involving data protection authorities.

On the EU Institutions' side, some EUIs are planning to implement manual contact tracing. The data collected in this processing operation includes the name and contact of the staff member who has been diagnosed with COVID-19, their place of work (number of the office and building floor of the staff member concerned), medical status of the staff member or of the household member with COVID-19 symptoms, result of the test (if applicable), time of onset of COVID-19 symptoms, as well as the list of close contacts with the staff member concerned over a period to be determined on a case-by-case basis after appearance of the first symptoms. The purpose of this manual contact tracing is to monitor the state of health of the staff, to verify the fitness to work and to implement social policies to promote staff's health and wellbeing. The data will only be disclosed to the concerned persons, their managers and to the employees in charge of doing the manual contact tracing. The name of the data subjects with COVID-19 and other necessary information may be disclosed to local health authorities, in line with national requirements. This manual contact tracing is planned to be mandatory.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Other decentralised approach.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

NIL.

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Major privacy risks: see answer 3.1

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

- Ensuring that national health authorities (or entities carrying out tasks in the public interest in the field of health) are the data controllers of the personal data;
- Ensuring that the individual remains in control, by underlining the **voluntary use of the application**, without any negative consequences for the individual who decides not to download/use the app. In terms of technology, the **Bluetooth Low Energy (BLE) technology** was considered the best approach as the communications between devices appears more precise, and therefore more appropriate, than for example the use of geolocation data (GNSS/GPS, or cellular location data), which would likely not work indoor, sometimes even outdoor, due to the limited precision;
- Defining a clear legal basis for the processing of personal data;
- Data minimisation;
- Limiting the disclosure/ access to personal data;
- Clear purpose limitation;
- Setting strict data retention periods;
- Ensuring the security of data;
- Ensuring the accuracy of the data;
- Involving data protection authorities.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

In March 2020, the EDPS was consulted by the European Commission on the use of telecommunications data for the monitoring of the spread of the COVID-19 outbreak. We replied through a letter underlining that data protection rules currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics, while also underlining the fundamental importance of data anonymisation, adequate data retention periods, data security and data access.

We have also issued a Technology dispatch on the functioning of Contact Tracing with Mobile Applications, aimed at explaining the functioning of contact tracing with mobile applications in a more comprehensive and user friendly way.

The EDPS is also a full member of the European Data Protection Board (EDPB), an independent European body established by the GDPR, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.

The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). The EDPB aims to ensure the consistent application in the European Union of the General Data Protection Regulation and of the European Law Enforcement Directive.

In this context, the EDPB was consulted by the European Commission regarding it guidance on contact tracing apps. Moreover, the EDPB has issued specific guidelines on the use of location data and contact tracing tools in the context of the Covid19 outbreak.

These guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:

- using location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures ;
- contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible.

Among the main recommendations, the EDPB underlined the fundamental importance of ensuring that every measure taken in these extraordinary circumstances is necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The EDPS has called for a pan-European approach and has underlined that the data and technology may be part of the solution, and by no means a "silver bullet". We have also recalled the importance of using data and technology as a tool to empower, rather than control, stigmatise or repress individuals and called for these measures deployed in times of crisis to be temporary by nature.

We have also underlined the importance of interoperability: any exit strategy that will provide more freedom to people's movements and remove travel restrictions must take into account that people will cross national borders. Any contact tracing application, if adopted, should be designed in a way to be able to operate and interact with different but similar applications.

As the supervisory authority for data protection of EU Institutions and Agencies, the EDPS will monitor the compliance of this processing operation with the applicable rules. The EDPS has requested clarifications on this processing operation and is in the process of providing recommendations

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

- Conducting of data protection / privacy impact assessment and other risk assessment prior to rolling out the contact tracing app, and regular audit and reassessment thereafter
- Minimisation of the collection and retention of personal data
- A decentralised approach to data storage and processing
- Prohibiting against misuse of personal data for incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy)
- Efficacy and effectiveness of the contact tracing app
- Termination of the contact tracing app and erasure of data collected by the app

4. Handling of children's or students' data in e-learning technologies

The EDPS has not dealt with this issue during the pandemic.

Gabon - National Commission for the Protection of Personal Data (CNPDCP)

1. ‘Health passports’
1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?
For cross-border/boundary travel Not yet, but it is being planned / considered by the government. *For domestic activities* Yes.
1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).
For domestic activities Name: Carnet Vaccinal (Vaccinal Record) Main purpose(s): To be deconfined and to move freely throughout the country Description: White booklet
1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.
For domestic activities Voluntary.
1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?
Rating (on a scale of 1 – 5): The problem does not arise in Gabon yet because we do not have one.
1.5 Please list out the personal data involved in the ‘health passport’ or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.
It is impossible to do this assessment because we do not have a health passport.
1.6 Is the data collected by the ‘health passport’ or similar measure(s) stored or processed in any central databases? Please elaborate.
No data is collected or stored.
1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the ‘health passport’ or similar measure(s)? What are the major privacy risks identified in the DPIA?
NIL.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
NIL.
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
NIL.
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
NIL.
1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?
NIL.
1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?
NIL.
1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
NIL.
1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.
NIL.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

NIL.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

NIL.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

NIL.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NIL.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

NIL.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No.

4. Handling of children's or students' data in e-learning technologies

NIL.

Georgia - The State Inspector's Service (SIS)

1. 'Health passports'
1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?
For cross-border/boundary travel Not yet, but it is being planned / considered by the government. *For domestic activities* Not yet, but it is being planned / considered by the government. **Comment:** "Health passports" or similar measure(s) are currently considered at the idea level in Georgia. The project of "COVID passport" related application/platform is at the initial stage of drafting and its main purposes and/or privacy risks cannot be fully identified at the moment. However, it shall be noted, that the State Inspector's Service was immediately involved at this stage in the consultation process and has provided potential developers/owners of the application with the general instructions/recommendations in accordance with the best International and European practice. Considering all of the above, the information in Section 1 is unfeasible to provide at the moment and will be available once the project of the application is finalized.
1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).
As noted in sub-section 1.1., precise information cannot be provided at the moment.
1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.
As noted in sub-section 1.1., precise information cannot be provided at the moment.
1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?
Comment: Provided that the project is at the initial drafting stage and main issues/characteristics are under consideration, the idea has not been yet communicated to the public. This can be assessed once the project will be finalized and available for public consultation.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.
As noted in sub-section 1.1., precise information cannot be provided at the moment.
1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.
Same applies in this section, these details cannot be provided at the moment.
1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?
As noted in sub-section 1.1., precise information cannot be provided at the moment.
1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
Yes. Considering the sensitivity and specific nature of the "health passport" and/or similar measures the State Inspector's Service certainly prioritizes it and once the system becomes operable it will be further reviewed and evaluated on a regular basis.
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
As per sub-section 1.1, the details cannot be provided at the moment. However, the developers/owners of the application/platform will be instructed in accordance with best International and European practice.
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
As per sub-section 1.1., specific regulations for cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions are not defined yet. However, according to the existing legislation of Georgia, in general, the transfer of data to other states and international organisations requires compliance with Articles 41 and 42 of the Law on Personal Data Protection. (Current version of mentioned Law is available in Georgian: https://matsne.gov.ge/ka/document/view/1561437?publication=22 Consolidated version (01/12/2016 - 22/03/2017) of mentioned Law is available in English: https://matsne.gov.ge/en/document/view/1561437?publication=9)

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

As mentioned in sub-section 1.1 and 1.2., these details cannot be identified for now. However, in any case, general principles provided for in Article 4 of the Law of Georgia on Personal Data Protection shall be observed during data processing:

- Data must be processed fairly and lawfully, without impinging on the dignity of a data subject;
- Data may be processed only for specific, clearly defined and legitimate purposes. Further processing of data for purposes that are incompatible with the original purpose shall be inadmissible;
- Data may be processed only to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which they are processed;
- Data must be valid and accurate, and must be updated, if necessary. Data that are collected without legal grounds and irrelevant to the processing purpose must be blocked, deleted or destroyed;
- Data may be kept only for the period necessary to achieve the purpose of data processing. After the purpose of data processing is achieved, the data must be locked, deleted or destroyed, or stored in a form that excludes identification of a person, unless otherwise determined by Law.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

As the supervisory authority, the State Inspector's service delivers consultations on data protection issues for private, governmental and non-governmental organisations, as well as for the individuals.

The Service is also authorised to provide legal opinions on legal acts in order to assess their compliance with personal data protection legislation. Thus, when the legal act is issued in relation to the "health passports" in Georgia, the Service will be the relevant body to provide official legal opinions and recommendations upon request.

In addition, the Service has the authority to monitor actual data processing operations by inspections/audits either its own initiative or during the examination of a citizen's complaint. It shall be noted that after the handling of a case which is followed by the issuance of a relevant decision, the Service is authorised to issue mandatory instructions under this decision that shall be observed by the data controller/data processor.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

As noted, precise information cannot be provided at the moment.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

As per sub-section 1.1 and 1.2., the details on the measures adopted in Georgian jurisdiction to address or mitigate the privacy risks associated with the development or use of "health passport" or similar measures (moreover real examples of it) cannot be provided at the moment.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19

Relevant regulations of Georgian legislation:
Ordinance of the Government of Georgia On the Approval of Isolation and Quarantine Rules can be accessed on the following link- https://matsne.gov.ge/en/document/view/4877009?publication=120

Decree of the Government of Georgia On the Approval of Measures to Prevent the Possible Spread of the Novel Coronavirus in Georgia and the Emergency Response Plan for Cases of Novel Coronavirus Disease - https://matsne.gov.ge/en/document/view/4821121?publication=34

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

The State Inspector's Service studied specific electronic systems, modules, platforms, where COVID-19 related information is processed.

For instance, in 2020 the Service inspected Covid-19 electronic test registration module (which also includes information on the health monitoring of incoming travelers and returning nationals) of National Center for Decease Control and Public Health and several data security risks were revealed - the preliminary passwords of users registered in this registration module were not changed; there was the lack of a two-level authentication mechanism posed a risk of privacy breach of information in the module, etc.

The Service issued mandatory instructions and tasked the Center: to ensure organizational-technical measures in order to avoid the usage of same account by two and/or more employees at the organization and ensure that all the employees authorized to access the module registered individually; at the same time the Center was instructed to activate two-factor authentication mechanisms for all users registered in the module; and to ensure a single activation of a request to the mandatory password change for already registered users.

In another case, during the temperature screening of citizens at the LEPL - Shota Rustaveli Tbilisi International Airport, the fact of unnecessary archiving of the temperature screening procedure (video material) was observed. In addition, several people had access to the temperature scanning system with the same user. Accordingly, video footage of citizens was collected and stored for a certain period without any need; Besides, it was impossible to identify an employee who had accessed the data.

After the inspection, the State Inspector's Service issued mandatory instructions. In particular, data controller was instructed to terminate achieving temperature screening procedure in the scanning system; to define a responsible person for administering a temperature screening, technical support, ensuring system security and erasure, access limitation of the users in the system and monitoring its activities and addressing them. Also, to elaborate mechanism, that ensures access to the temperature scanning system via individual and personalized user and password.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

As per section 1.11, all general principles apply in this case. Namely, the principles provided for in Article 4 of the Law of Georgia on Personal Data Protection must be observed during data processing:
a) Data must be processed fairly and lawfully, without impinging on the dignity of a data subject;
b) Data may be processed only for specific, clearly defined and legitimate purposes. Further processing of data for purposes that are incompatible with the original purpose shall be inadmissible;
c) Data may be processed only to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which they are processed;
d) Data must be valid and accurate, and must be updated, if necessary. Data that are collected without legal grounds and irrelevant to the processing purpose must be blocked, deleted or destroyed;
e) Data may be kept only for the period necessary to achieve the purpose of data processing. After the purpose of data processing is achieved, the data must be locked, deleted or destroyed, or stored in a form that excludes identification of a person, unless otherwise determined by Law.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

As per sub-section 1.12 of this questionnaire, as the supervisory authority, the State Inspector's service delivers consultations on data protection issues for private, governmental and non-governmental organisations, as well as for the individuals. The Service is also authorised to provide legal opinions on legal acts in order to assess their compliance with personal data protection legislation.

The Service also monitors actual data processing operations by inspections/audits either its own initiative or during the examination of a citizen's complaint. After the handling of a case which is followed by the issuance of a relevant decision, the Service is authorised to issue mandatory instructions under this decision that shall be observed by the data controller/data processor.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

As mentioned in the sub-section, the Service issued mandatory instructions and tasked the Center: to ensure organizational-technical measures in order to avoid the usage of same account by two and/or more employees at the organization and ensure that all the employees authorized to access the module registered individually; at the same time the Center was instructed to activate two-factor authentication mechanisms for all users registered in the module; and to ensure a single activation of a request to the mandatory password change for already registered users.

In another case, the data controller was instructed to terminate achieving temperature screening procedure in the scanning system; to define a responsible person for administering a temperature screening, technical support, ensuring system security and erasure, access limitation of the users in the system and monitoring its activities and addressing them. Also, to elaborate mechanism, that ensures access to the temperature scanning system via individual and personalized user and password.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Apart from the legal requirements, observance of the recommendations and mandatory instructions of the State Inspector's Service can be considered as relevant measure.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No.

Primarily, it shall be noted that the contract tracing application has been deactivated at the moment in Georgia. It has been operable during several months and at the initial stage of the application development the State Inspector's Service has issued recommendations. Thus, information in this section is given in accordance to the past experience on this digital contact tracing app.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?

- Bluetooth technology
- GPS location tracking
- Others

As noted in section 3.1., above, the application is not operable at the moment. However, according to the Ministry of Internally Displaced Persons from the Occupied Territories, Labor, Health and Social Affairs of Georgia, in order to identify which devices were in close contact, the application used Bluetooth, location (however, according to the Ministry, location data are not processed by this app) and Google Nearby technologies.

What best describes the approach used to build the contact tracing app?
Other decentralised approach.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

In April, 2020, at the initiative of the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia, a mobile application **"Stop COVID"** was introduced in the country. The aim of the application was an early detection and prevention of COVID-19 cases. It helped users to determine whether they had any contact with a person infected with COVID-19 (i.e. a person who also have downloaded and activated the application).

The use of the application depended on the free will of the user. In order to identify which devices were in close contact, the application used Bluetooth, location (however, according to the Ministry, location data are not processed by this app) and Google Nearby technologies.

Information on the interaction between users of application (i.e. date of the contact, duration (more than 15 minutes) and distance (less than 2m)) were stored locally in a relevant mobile device of the users in contact. If any of them were confirmed positive of Covid-19, he/she could inform persons interacted with him/her by marking relevant option in the application. The procedure of the notification was the following: after pressing relevant button, a form for mobile phone number would appear. Subsequent to providing phone number, a one-time PIN code was sent to this number for verification purposes. This number was then

checked at the database of infected persons of National Center for Disease Control and Public Health. If the owner of the phone number was confirmed of Covid-19, the notification of the user in the application would be approved. Upon confirmation, the user would agree or deny sharing information about the contacts within last 5 days. As a result, these persons in contact with the infected within last 5 days would receive notice alongside the relevant instruction through the application.

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

According to the existing legislation of Georgia, conducting a DPIA is not mandatory. However, upon the announcement of launch of new contact tracing application, the State Inspector's Service immediately addressed the Ministry for details and issued relevant recommendations.

Major privacy risks as identified by the State Inspector's Service within a consultation process, were following:

- Ambiguousness in the data confidentiality statement
- Possibility to demand erasure of data by the data subject
- Aims of data processing and data storage period
- Using updated protocol of Apple Bluetooth operation for IOS system mobile devices
- Periodic change of Unique Identifier of the user
- Availability of program number of the application

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

According to Georgian practice, key data protection principles regarding the development and use of contact tracing application were **lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity and confidentiality (security).**

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

As noted in the sub-section 1.12., as the supervisory authority, the State Inspector's service delivers consultations on data protection issues and provides legal opinions on legal acts in order to assess their compliance with personal data protection legislation.

As the „STOP COVID"application operated in a short period of time, its data processing operations could not be inspected. However, at the initial stage, the State Inspector's Service provided recommendations and delivered consultations regarding the best data protection practices to be considered.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Taking into account the European countries' best practices, the Service has prepared and submitted recommendations to the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia on the following issues: clear definition of data processing objectives and timeframe for storing in the application; correction of ambiguities in the data confidentiality statement; enabling data subject to request deletion of his/her data; accessibility to the application software code and other technical issues. The purpose of the recommendations was to bring data processing through the application in line with the law and gain public trust towards the application.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

- Minimisation of the collection and retention of personal data;
- A centralised or decentralised approach to data storage and processing;
- Prohibiting against misuse of personal data for incompatible purposes;
- Data security measures (e.g. encryption, decentralised data processing, etc.);
- Transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy);
- Termination of the contact tracing app and erasure of data collected by the app;

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

For Distance learning processes - „Google meet" and „Zoom cloud meeting"
Also, for an electronic journaling – so called "school book" platform has been used.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

As mentioned above, conducting DPIA is not mandatory according to the existing legislation. However, as the State Inspector's Service inspected 4 schools (public and private) and 4 Universities, it had also an opportunity to observe the processes and issue relevant recommendations.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

For instance, an e-journal was used during the distance learning process in several public schools, which did not register some operations performed in relation to the student data; Private schools did not have mechanisms for students' personal data protection during the distance learning (for example, the school did not have rules and conditions for access to electronic data, which would enable the proper monitoring of authorised data processing by employees, as well as the proper response to the revealed offences);

The Service also examined lawfulness of processing student data by the LEPL - Office of Resource Officers of Educational Institutions through the unified electronic database - erofcers.emis.ge. This database contains information on violations and/or alleged violations by 549,000 students in 607 public schools, namely: student name, surname, personal number, gender, social status (protected/vulnerable),
class, school, citizenship, region, district, date of birth, telephone number and address (legal/actual); Name/surname, personal number, telephone number, address, date of birth and information about the employment of the parent/representative; Category of the offence committed by the student (possession of prohibited items, alcohol, consumption of tobacco products, gambling, etc.); Type of violation (possession of a cold weapon, truncheon or poisonous substance, etc.); Content of the violation (time, place); Measures taken by the resource officer/authorized person; Persons involved in the incident and others. In the same information base, the main data of students and their legal representatives are generated from the electronic platform of LEPL Education Management Information System - eSchool (a unified platform, which contains the identification data of persons enrolled in schools across Georgia, information on their academic performance, educational activities, etc.).

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

As noted above, general principles provided for in Article 4 of the Law of Georgia on Personal Data Protection shall be observed also in these cases:

a) Data must be processed fairly and lawfully, without impinging on the dignity of a data subject;
b) Data may be processed only for specific, clearly defined and legitimate purposes. Further processing of data for purposes that are incompatible with the original purpose shall be inadmissible;
c) Data may be processed only to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which they are processed;
d) Data must be valid and accurate, and must be updated, if necessary. Data that are collected without legal grounds and irrelevant to the processing purpose must be blocked, deleted or destroyed;
e) Data may be kept only for the period necessary to achieve the purpose of data processing. After the purpose of data processing is achieved, the data must be locked, deleted or destroyed, or stored in a form that excludes identification of a person, unless otherwise determined by Law.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

As mentioned above, with respect to handling of children's or students' data in the use of e-learning technologies, the State Inspector's Service inspected 4 schools (public and private) and 4 Universities and issued relevant recommendations.

After examining the lawfulness of processing student data by the LEPL - Office of Resource officers of Educational Institutions through the unified electronic database - erofcers.emis.ge, the Service issued some mandatory instructions: to ensure organizational and technical measures which will enable documenting all the activities on the data in electronic journal. Also, to develop instructions for students' data processing via electronic journal, where specific periods for data storage will be also included.

At the same time, schools that were using "teams" were instructed to ensure a mechanism, that will enable employees at the school to document students' data in a non-automatically and to operate according to the unified rules established by the school. The measures shall ensure timely and secure destruction of the data after achieving relevant goals.

Besides, school was also recommended to elaborate rules/instructions in order to define data protection issues in the distance learning process.

The universities were instructed to assess and determine data storage periods, also to document log data (where necessary) and establish the automatic mechanism for data erasure.

4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.

Apart from the legal requirements, observance of the recommendations and mandatory instructions of the State Inspector's Service can be considered as relevant measures in this regard. For instance, recently the Service was notified that:

- According to the Order of the School principal the form of schoolbook was adopted for distance learning. All the teachers were tasked to fill this form and were notified about the rules of its storage and the limitations of revealing the information;
- Schools elaborated and issued the monitoring mechanisms and regulations for the protection of data of employees, pupils and parents. This document describes in detail: the types of data processed at school, means of their processing, purposes of their usage, persons responsible for their access, data protection and its monitoring procedures;

One of the Schools has issued an individual legal act under which the persons responsible for the monitoring of data protection were defined. They were tasked to monitor regularly data processing by teachers; to address the revealed violations, as well as to conduct informational meetings with the employees and pupils in order to inform them on personal data protection issues and related measures.

Germany - Federal Commissioner for Data Protection and Freedom of Information of Germany (BfDI)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: EU Digital COVID Certificate
Main purpose(s): see website
Description: see website
Link to website: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

For domestic activities
Name: EU Digital COVID Certificate
Main purpose(s): see website
Description: see website
Link to website: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

Details (if applicable): Using the health app is voluntary. For some situations, it is mandatory to provide a health certificate (proof of negative test result, vaccination or recovery), this can be done either by showing a paper (hardcopy), pdf-file or by using the “health passport” app (this will be, in most cases, more convenient for users).

For domestic activities
Voluntary.

Details (if applicable): Using the health app is voluntary. For some situations, it is mandatory to provide a health certificate (proof of negative test result, vaccination or recovery), this can be done either by showing a paper (hardcopy), pdf-file or by using the “health passport” app (this will be, in most cases, more convenient for users).

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 5

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: name, birth date, vaccination/testing or recovery date, vaccine or test product
Parties having access to the data: data subject, partly border control

For domestic activities
Personal data involved: name, birth date, vaccination/testing or recovery date, vaccine or test product
Parties having access to the data: data subject, partly admission control

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
Data breaches, ransom attacks, misfunctioning or encryption, etc.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

No.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.

Details: The EU Digital COVID Certificate is temporally until the WHO declares the Corona pandemic to be ended.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

Gateway provided by the EU-Commission for all EU-Members

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

The EU Digital COVID Certificate is in accordance to the GDPR of the EU.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

We closely monitored the implementation.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

See: https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opiniondigital-green-certificate_en

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

See: https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opiniondigital-green-certificate_en

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

As of now (12 July 2021) it depends on the country of origin of travellers (if they come from a "riks area", "high incidence area" or a "virus variant area") and on the means of travel. Incoming flight passengers always need to have a negative test result (Antigen test taken max. 48h before arrival in Germany, PCR test taken max. 72h before arrival)), or proof of full vaccination or recovery before flying to Germany.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Storage of personal data and discrimination.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

See GDPR - https://gdpr.eu/
As well as Coronavirus-Einreiseverordnung - https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/guv-19-lp/coronaeinreisev.html (translation not applicable)

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Monitoring of the legislation.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Not applicable.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Not applicable.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Corona-Warn-App
Description: see webiste
Link to website:
https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-appenglisch

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

Details: The use of the app is based on the consent of the data subject.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
Identification of users by the Exposure Notification API builders and app-store owners Google and Apple. Bugs in the BLE environment and building social graphs by scanning BT-signals in open places (see FiFF DPIA, "Angriff B2").

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Open-source, decentralised, pseudonym.
See website.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

We closely monitored the implementation and consultation of the data controller (Robert-Koch-Institut)

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Conducting of data protection / privacy impact assessment and other risk assessment prior to rolling out the contact tracing app, and regular audit and reassessment thereafter.

4. Handling of children's or students' data in e-learning technologies

This section is completed by subnational DPAs of Germany: Data Protection and Freedom of Information Commissioner of Berlin and the Data Protection Commissioner of Thuringia.

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Preliminary Remark: Please note that schools and education affairs in Germany are under responsibility of federal states, due to the federal system in Germany. Two DPAs of federal states, DPA of Berlin and DPA of Thüringen/Thuringia (both are sub-national members of GPA) have provided answers to this section.

Berlin:
The Berlin Ministry of Education has been developing an e-learning platform since 2005 that was used by several schools before. With the start of the pandemic in 2020 the use of this platform has increased

significantly. We have no information about all e-learning technologies used by the schools. We know e. g. about the use of "itslearning" and "iserv" but since the schools choose the applications there is a wide range of different platforms in use.

Thuringia:
E-Learning Platforms, very often the Thüringer Schulcloud (Thuringian School Cloud), which is based on the Schul-Cloud des Hasso-Plattner-Instituts (Hasso Plattner Institute´s School Cloud).
The Moodle platform is used less frequently.
In addition, the video conferencing systems BigBlueButton and less frequently Jitsi Meet are used.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Berlin:
Yes.

Thuringia:
Yes, of course, with the TLfDI carrying out an initial cursory examination upon request.
However, the schools are controllers under Article 4(7) GDPR

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Berlin:
The major findings regarding privacy risks are: 1) missing routines regarding the deletion of personal data of children and teachers, 2) missing client separation, 3) processing of personal data outside of e-learning platforms and 4) the use of platforms that violate the GDPR.

Thuringia:
The major privacy risks are the unauthorised use of other school platforms, e.g. from the USA, and software products without prior examination under data protection law.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Berlin:
Due to the absence of a legal framework for using e-learning technologies in schools in Berlin, it is necessary that users (parents on behalf of their children or adult pupils) get informed and give their consent freely. The consent has to be in accordance with the requirements of the GDPR for using these technologies. Schools have to ensure that all children are also able to receive material necessary for their participation in school lessons via alternate means if no consent is given. It is necessary to ensure that personal data is only processed for specific and explicit purposes of the specific e-learning technology, and – without explicit consent – not for e. g. research purposes. Personal data has to be deleted as soon as it is no longer necessary. At the end of the school year personal data saved within the e-learning platforms has to be deleted by default.

Thuringia:
It would be desirable if the federal state provided e-learning technologies to the schools, e.g. running on the state's own servers. These could then be checked by the data protection supervisory authority in good time before they are used. Students must receive precise instructions on how to use the products.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Berlin:
In April 2020 we published compliance guidelines regarding data protection of e-learning platforms used by schools in Berlin. Key points are requirements for informed consent that is compliant with the GDPR, technical requirements to ensure a minimum level of security and risk management and requirements for data processing agreements.
The guidelines are available at:
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDILernplattformen_Hinweis.pdf

Thuringia:
There is a is guidebook from the data protection supervisory authority for online learning platforms in school classrooms:
https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/guidebook_from_the_data_protection_supervisory.pdf
Note: The English version of the "Guidance of the data protection supervisory authorities for online learning platforms in school classrooms" adopted by the Data Protection Conference was translated at the request of the Thuringian State Commissioner for Data Protection and Freedom of Information.

4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.

Berlin:

- Assessment of privacy impact or risk assessment by schools (PIA)
- Assessment of the necessity, effectiveness and proportionality of exam monitoring measures and tools
- Implementation of the appropriate data security measures for and within the e-learning tools
- Implementation of adequate safeguards for cross-border transfer of personal data collected by elearning tools
- Policies forbidding the recording of audio and video of lessons by default
- Provision of guidance to parents

Thuringia:

- Assessment of privacy impact or risk assessment by schools
- Implementation of the appropriate data security measures in the e-learning tools
- Policies regarding the recording of audio and video of lessons
- Provision of guidance to parents and the students

Gibraltar - Gibraltar Regulatory Authority (GRA)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: Vaccination Confirmation Certificate
Main purpose(s): Proof of an individual’s vaccination status for travelling abroad.
Description:
Gibraltar residents who are required to provide proof of their vaccine status abroad can request a Vaccination Confirmation Certificate from the Gibraltar Health Authority. The certificate can be kept as a permanent record of an individual’s vaccination status, to be used for all travel (subject to being recognised by international organisations/jurisdictions).
Link to website: https://healthygibraltar.org/news/covid-19-certificates/

Name: Travel Certificate
Main purpose(s): Proof of a rapid antigen test for travelling abroad.
Description:
Passengers travelling to an airport or country that permits the use of rapid antigen tests may do so at the Covid Rapid Test facility at the Gibraltar International Airport. They would then be provided with a Travel Certificate.
Link to website: https://healthygibraltar.org/news/covid-19-certificates/

For domestic activities
Name: Gibraltar Covid-19 Vaccination Record
Main purpose(s): Provides proof of vaccinations.
Description:
Once an individual receives both doses of their Covid-19 vaccination, they are provided with the Gibraltar Covid-19 Vaccination Record (an ID card / driver’s licence card style format) as proof of vaccination.
Link to website: Not applicable

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

Details (if applicable):
While the Vaccination Confirmation Certificate and Travel Certificate are not mandatory, they may be required for access to certain jurisdictions at the discretion of said jurisdictions.

For domestic activities
Voluntary.

Details (if applicable):
The Gibraltar Covid-19 Vaccination Record does not act as a 'health passport', however, some ticketed social events held locally have been required by the public health authorities to request proof of vaccination prior to allowing entry to the event. Should an individual not be able to provide a Covid-19 Vaccination Record card, they are required to take and produce a negative lateral flow test on the day of the event. Refusal to provide either the Covid-19 Vaccination Record card or a negative lateral flow test would result in access being denied to an event.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 4

Whilst our authority has not received concerns from the public in relation to such documents, anecdotal evidence shows that that has not been overwhelming objection to the measures.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved:

- Full name
- Date of Birth
- Passport copy
- Gibraltar Health Authority Number
- Email
- Telephone number
- Gibraltar Covid-19 Vaccination Record card copy

Parties having access to the data: Public Health Gibraltar

For domestic activities
Personal data involved:

- Full name
- Date of Birth
- Date of Vaccinations
- Gibraltar Health Authority number

Parties having access to the data: Gibraltar Health Authority

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Our authority does not have relevant information to explicitly confirm this.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Our authority does not have details on whether a DPIA has been conducted.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Our authority does not have details of whether such review and evaluation are planned.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Our authority is currently unaware of any plans in place for the termination of health passports after the Covid-19 pandemic is over.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

Our authority does not have relevant information to explicitly confirm this.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Such principles would relate to those as found in Article 5 of the Gibraltar General Data Protection Regulation ("Gibraltar GDPR"), namely that personal shall be processed:

1. lawfully, fairly and in a transparent manner in relation to the data subject;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. processed in a manner that ensures appropriate security of the personal data.

Additionally, such processing would require a lawful basis as per Article 6 of the Gibraltar GDPR and in relation to health data, as a special category of personal data, a further condition under Article 9(2) of the Gibraltar GDPR.

Further, such measures should have adhered to the principles of Privacy by Design and Privacy by Default, as per Article 25 of the Gibraltar GDPR.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

The Gibraltar Regulatory Authority is the independent statutory body responsible for the enforcement of data protection legislation in Gibraltar, and carries out the functions assigned to it, to uphold the rights of individuals and their privacy. We had no involvement in relation to the planning or implementation of such measures but have powers to investigate any possible breaches and issue advice and guidance in relation to compliance with data protection legislation.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The Gibraltar Regulatory Authority has not specifically published any guidance or advice relating to such matters. However, the following guidance has been published in relation to Covid-19 measures:

- Guidance note relating to the Covid-19 pandemic. It is titled "GDPR & DPA (20) Covid-19 Temperature Checks". It is available at https://www.gra.gi/data-protection/guidance/gdpr-dpa-20-covid-19-temperature-checks. Press release relating to the same is available at https://www.gra.gi/data-protection/press-releases/covid-19-temperature-checks.
- Guidance note titled "GDPR & DPA (19) Covid-19: Contact Tracing & Location Data". It is available at https://www.gra.gi/data-protection/gdpr-dpa-19-covid-19-contact-tracing-location-data-.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

Processing should comply with the requirements of the Gibraltar GDPR and we would expect a DPIA to have been carried out before such processing, as required in the circumstances as set out under Article 35(3) of the Gibraltar GDPR, given that such processing is likely to result in a high risk to data subjects.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities
- Others, please provide a brief description:

Depending on whether they are arriving from a Green, Amber or Red list country (as per the Gibraltar COVID-19 related regulations, e.g. Civil Contingencies Emergency (Coronavirus) (Requirements on entry into Gibraltar and Testing)(No.3) Regulations 2021), and whether they are vaccinated or not, individuals may need to complete a passenger locator form before arrival, upload a vaccination certificate or present one upon arrival, conduct a lateral flow test on arrival or 24 hours after arrival, and conduct a further lateral flow test 5 days after arrival, or quarantine.

Please see Annex A to this document at https://www.gibraltar.gov.gi/press-releases/updates-to-covid-19-

testing-and-self-isolation-requirements-for-travel-to-gibraltar-4502021-7017, which lists the full requirements for entry, including the monitoring of health of individuals.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

In first instance, our authority identifies the security of the data as a priority but has also identified other areas such as retention and purpose limitation.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

As per Article 5 of the Gibraltar GDPR, ensuring personal data is processed:

1. lawfully, fairly and in a transparent manner in relation to the data subject;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. processed in a manner that ensures appropriate security of the personal data.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

No role in relation to the planning or implementation of such measures. We would however investigate any complaints/concerns that we become aware of.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Although not specific to health monitoring of incoming travellers and returning nationals, please refer to the guidance noted in response to question 1.13 above.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

See response to 1.14 above.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Beat COVID Gibraltar

Description:
The Beat COVID Gibraltar App uses the bluetooth technology on a user's phone to track other phones the user has been in close proximity to. It uses the Exposure Notification Service and the user will be notified directly if they have been in close contact with someone who has tested positive for the virus. Likewise, if the user tests positive for Covid-19, those they have been in close contact with, will be notified.

Link to website: https://www.gibraltar.gov.gi/beatcovidapp

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.

Link to relevant legislation:
https://www.gibraltarlaws.gov.gi/legislations/civil-contingencies-emergency-coronavirus-passenger-locator-form-no11-regulations-2021-6132 - regarding passenger locator forms for air travel.

https://www.gibraltarlaws.gov.gi/legislations/civil-contingencies-emergency-coronavirus-businesses-restrictions-and-other-matters-no4-regulations-2021-6127 - see in particular section 8(8) regarding restaurant/bar/cafe contact tracing:

> *8.(1) A person responsible for carrying on a business of a restaurant, cafeteria or bar where food or drink is sold for consumption on the premises requires a permit from the Director of Public Health.*
>
> *8.(8) A person referred to in subregulation (1) must- (a) keep a daily list of the name and contact telephone number of all the customers who have booked a table at the restaurant, cafeteria or bar; (b) keep such list for 10 days from the date for which the table was booked; (c) where the Director of Public Health requests a copy of the daily list for a particular day for contact tracing purposes, that list must be provided to the Director of Public Health without undue delay.*
>
> *9.(9) The list referred to in subregulation (8) must be destroyed at the end of the 10 days after the date for which the table was booked.*

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

It is not known if a DPIA has been conducted, although it is expected that one should have been undertaken. The major of privacy risks are similar to those identified in 2.3 above.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Please refer to the answer to question 1.11 above.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

As per response to 3.4. We have issued ad-hoc advice in relation to contact tracing generally, and issued a guidance note (as set out below.)

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

GDPR & DPA Covid-19: Contact Tracing & Location Data (link to guidance note)

This guidance note provides information and guidance in respect of the rapid developments in the use of technology to support the fight against Covid-19, in particular technology to 1) trace contact amongst the population, and 2) map the spread of the virus. It is not specific to the App.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Our authority has issued guidance to assist in compliance with data protection legislation.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Seesaw and Google Classroom.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Not specifically in relation to e-learning technologies, however as per Article 35(3) of the Gibraltar GDPR, a DPIA is required in the case:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data (as defined in Article 9(1) of the Gibraltar GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 of the Gibraltar GDPR; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

Should such processing fall into the above categories, a DPIA would be required.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

The risks would be similar to those identified in 2.2 above.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Please refer to the answer to question 1.11 above.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Our authority has not yet published guidance on e-learning technologies but there are plans for this to be published.

4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.

Such processing should comply with the requirements of the Gibraltar GDPR.
Guidance on the matter is currently being developed.

Hong Kong, China - Office of the Privacy Commissioner for Personal Data (PCPD)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name:
(i) Return2hk Scheme (Currently the scheme is implemented for Hong Kong residents returning from the Mainland of China or Macao, not for ‘international travel’. It is classified as a ‘health passport’ for international travel only for the purpose of this survey in order to ensure consistency with the classification of ‘health passports’ in other jurisdictions.)
(ii) Boarding and Compulsory Quarantine Arrangements for Persons Arriving in Hong Kong from Places Outside China (no official ‘health passport’ under the arrangement)

Main purpose(s):
(i) Return2hk Scheme: To exempt Hong Kong residents from the 14-day compulsory quarantine requirement when returning to Hong Kong SAR from the Mainland of China or Macao SAR.
(ii) The arrangement aims to tighten the border control measures for overseas inbound travellers based on "vaccine bubble" in order to build an anti-epidemic barrier to prevent the importation of COVID-19 cases.

Description:
(i) Under the Return2hk Scheme, Hong Kong residents may return to Hong Kong SAR from the Mainland or Macao SAR without being subject to the 14-day compulsory quarantine requirement, provided that certain conditions are met. The returning Hong Kong residents must first undergo COVID-19 nucleic acid test within 3 days before returning to Hong Kong and provide test results. For those residents returning to Hong Kong SAR from Guangdong Province or Macao SAR via land boundary control points, they are strongly advised to transfer their negative COVID-19 test results electronically from the health code systems of Guangdong (namely the Yuekang Code) or Macao SAR (namely the Macao Health Code) to the electronic health declaration system of Hong Kong SAR’s Department of Health (namely Hong Kong Electronic Health Declaration Form) in order to expedite the clearance process. A unique QR code will be generated by the Hong Kong Electronic Health Declaration Form system upon successful transfer of information. The QR code will be shown to the staff of the Department of Health at Hong Kong ports for clearance. If a returning Hong Kong resident who does not have a smartphone, or if he/she returns via the Hong Kong International Airport, a paper copy of the original COVID-19 testing record will also be accepted.

Link to relevant website: https://www.coronavirus.gov.hk/eng/return2hk-scheme.html

(ii) Currently, all people coming to Hong Kong from places outside Guangdong Province of China have to present negative results of COVID-19 test conducted within 72 hours (3 days for Mainland China except Guangdong Province) before the scheduled time of the aircraft. For persons having stayed in high-risk specified places during a relevant period, they have to present recognised vaccination records as an additional requirement for boarding the flight. All these people will still have to undergo compulsory quarantine for a period of 21/14/7 days upon arrival, depending on the risk level of the places they have stayed and whether they can present the required vaccination record.

Link to relevant Government's press release:
https://www.info.gov.hk/gia/general/202108/03/P2021080200985.htm
https://www.coronavirus.gov.hk/eng/inbound-travel.html

For domestic activities
Name:
Vaccine Bubble Scheme

Main purpose(s):
To relax social distancing measures and other restrictions for vaccinated people.

Description:
Under the Vaccine Bubble Scheme launched by the Government of Hong Kong SAR, certain premises (e.g. bars, pubs, cruise ships and other catering businesses under certain modes of operation) can only assign vaccinated staff members to be on duty. Furthermore, some of these premises can only admit vaccinated customers. For staff/customers who are unfit to receive vaccination because of health reasons, those who are aged 16 or above must duly complete a declaration form and present a medical certificate, as well as the negative result of a COVID-19 test received within the preceding three days. Staff/customers may present their vaccination records or COVID-19 test results in paper or electronic format (affixed with a unique QR code except the paper COVID-19 test results) to premises operators. A "QR Code Verification Scanner" app was developed by the Government specifically for premises operators to scan the QR codes affixed on the vaccination records or COVID-19 test results of their customers/staff for checking whether the customers/staff have complied with the relevant requirements about COVID-19 vaccination and testing.

Link to relevant websites:
- Vaccine Bubble Scheme:
  https://www.info.gov.hk/gia/general/202104/28/P2021042800868.htm?fontSize=1
  https://gia.info.gov.hk/general/202107/21/P2021072100493_372915_1_1626845692806.pdf
- QR Code Verification Scanner app:
  https://www.fehd.gov.hk/english/events/covid19/vaccination_record_app.html

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Mandatory.

Details (if applicable):

Under the Prevention and Control of Disease (Regulation of Cross-boundary Conveyances and Travellers) Regulation (Cap. 599H), anyone who boards a flight for Hong Kong from places outside Guangdong Province of China has to present prior to boarding a negative result proof of a polymerase chain reaction (PCR)-based nucleic acid test for COVID-19 the sample for which was taken within 72 hours (3 days for Mainland China except Guangdong Province) before the scheduled time of departure of the aircraft; for persons having stayed in high risk specified places during a relevant period, they have to present recognised vaccination records as an additional requirement for boarding the flight.

- Chapter 599H, Laws of Hong Kong: https://www.elegislation.gov.hk/hk/cap599H!en-zh-Hant-HK?INDEX_CS=N

For domestic activities
Mandatory.

Details (if applicable):
Pursuant to the directions and specifications issued by the Government under the Prevention and Control of Disease (Requirements and Directions) (Business and Premises) Regulation (Chapter 599F, Laws of Hong Kong), vaccination and/or COVID-19 test results are required for operating or patronising certain premises.

- Government press release about the Vaccine Bubble Scheme: https://www.info.gov.hk/gia/general/202104/28/P2021042800868.htm?fontSize=1
- Arrangements for Cap. 599F Premises under the "Vaccine Bubble": https://gia.info.gov.hk/general/202107/21/P2021072100493_372915_1_1626845692806.pdf

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): We do not have sufficient information to assess the public acceptance of the idea of 'health passport' in Hong Kong at the time of responding.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved:
The boarding requirements under Cap 599H will involve the following types of personal data:

- Full name;
- Sex;
- Date of birth;
- Identity card/passport/travel document number; and
- COVID-19 PCR test result.

A vaccination certificate contains the following types of personal data:

- Name;
- Date of birth;
- Identity card/passport number;
- Date of vaccination; and
- Vaccine name.

Parties having access to the data:
The Department of Health and the Office of Government Chief Information Officer of the Hong Kong SAR Government.

For domestic activities
Personal data involved:
A vaccination certificate contains the following types of personal data:

- Name;
- Identity card number;
- Date of vaccination; and
- Vaccine name.

A COVID-19 testing record contains the following types of personal data:

- Identity card/passport/travel document number;
- Test result/report date;
- Specimen collection date;
- Specimen type;
- Testing platform; and
- Test result.

Parties having access to the data:
The Department of Health, the Hospital Authority and the Office of Government Chief Information Officer of Hong Kong SAR, as well as the vaccination/testing centres, and staff of the designated premises (view only).

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details:
Information about vaccination status and COVID-19 test results used for the Return2hk Scheme and Vaccine Bubble Scheme is stored centrally in the systems of the Hong Kong SAR Government.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

The PCPD separately provided its general observations in relation to the Return2hk Scheme, Hong Kong Health Code and the local Vaccine Bubble Scheme from the personal data protection perspective for the Government's consideration.

Major privacy risks:
Not disclosed.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Unknown to the PCPD.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Unknown to the PCPD.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

Currently, under the Return2hk Scheme, returning Hong Kong residents can transfer, with their knowledge and consent, their COVID-19 test results from the Yuekang Code or Macao Health Code system of the Guangdong/Macao authority to the Hong Kong Electronic Health Declaration Form system for generating a QR code for entering Hong Kong. The returning Hong Kong residents may also present a paper-based copy of their COVID-19 test results to the staff of Hong Kong SAR's Department of Health at the boundary control points.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Purpose specification: The purpose for which personal data will be used should be made clear to the data subjects (e.g. to facilitate cross-border travels during the pandemic).

Data minimisation: Only minimum amount of necessary personal data should be collected for fulfilling the specified purpose.

Transparency: The policies and practices in relation to the processing of personal data should be disclosed to the public.

Accuracy: Personal data, including vaccination status and COVID-19 test results, shall be accurate and up to date.

Use limitation: Personal data shall only be used for the original purpose of collection.

Data security: Personal data shall be protected against unauthorised or accidental access, processing, erasure, loss or use.

Retention limitation: Personal data shall not be kept longer than is necessary for fulfilling the purpose of collection.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

The PCPD previously provided its observations in relation to the Return2hk Scheme and the local Vaccine Bubble Scheme from the personal data protection perspective for the Government's consideration.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

In sharing its observations with the Government, the PCPD mainly reiterated the importance of adhering to the data protection principles in Schedule 1 to the Personal Data (Privacy) Ordinance (PDPO, Chapter 486 of the Laws of Hong Kong) in the implementation of the relevant initiatives, which are summarised below:

- Only the minimum, necessary and non-excessive personal data should be collected;
- Data users should be transparent about and explain clearly, inter alia, the purpose for which the personal data is to be used, the classes of persons to whom the personal data may be transferred, etc.;
- Personal data shall not be retained for longer than is necessary for fulfilment of the purposes (including any directly related purposes) for which the data is or is to be used;
- The personal data shall not be used for any new purposes unless the prescribed consent from a data subject is obtained or when any of the statutory exemption under Part 8 of the PDPO applies;
- Personal data collected must be protected with appropriate safeguards and security measures against unauthorised or accidental access, processing, erasure, loss or use; and
- Data subjects are entitled to request access to and correction of the personal data concerned.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

The Government of Hong Kong SAR provides 'local vaccine bubble version' of the electronic vaccination records for individuals to download and use under the Vaccine Bubble Scheme. The 'local vaccine bubble version' of an electronic vaccination records has the name and identity card number of the data subject partially masked to protect personal data privacy.

In an electronic COVID-19 testing record issued to the data subject, the identity card/passport number/travel document of the data subject is partially masked. Name or other personally identifiable information of the data subject is not included.

Both the vaccination record and the COVID-19 testing record are affixed with a unique QR code to indicate the vaccination status or test result of the data subject, except the paper testing result record. The "QR Code Verification Scanner" app was developed by the Government for premises operators to scan the QR codes. By using the app to scan the QR codes, no personally identifiable information will be shown, but only the vaccination status or test results. Under the Vaccine Bubble Scheme, premises operators are required to use the app to scan the QR codes on the vaccination records and the COVID-19 testing records for verification. The app helps to protect personal data privacy of the data subjects.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities
- Others:
  Some incoming travellers and returning Hong Kong residents may be allowed to undergo quarantine at home if certain conditions are met. These people will be required to install the "StayHomeSafe" app and wear electronic wristbands to ensure that they complete their quarantine period at home.

  In addition, incoming travellers and returning Hong Kong residents may have their compulsory quarantine periods shorten if they can present vaccination records.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Data security: Health monitoring involves collection of sensitive health data, which may be attractive to hackers. As sensitive data is involved, the harm that may be caused by a data breach is greater.

Misuse of personal data: Personal data may be used for purposes other than health monitoring.

Duration of retention: The risk of personal data being retained longer than the period necessary for achieving the purpose of health monitoring. This will increase the risks of data breach and misuse.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Purpose specification: The purpose for which personal data will be used should be made clear to the data subjects (e.g. to ensure that incoming travellers and returning Hong Kong residents do not carry COVID-19 virus).

Data minimisation: Only minimum amount of necessary personal data should be collected for fulfilling the specified purpose.

Transparency: The policies and practices in relation to the processing of personal data should be disclosed to the public.

Accuracy: Personal data, including vaccination status and COVID-19 test results, shall be accurate and up to date.

Use limitation: Personal data shall only be used for the original purpose of collection.

Data security: Personal data shall be protected against unauthorised or accidental access, processing, erasure, loss or use.

Retention limitation: Personal data shall not be kept longer than is necessary for fulfilling the purpose of collection.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

The PCPD shared its views as to the Government's health quarantine measure (including the attachment of a wristband to a confinee which is connected with a mobile app to assess if the confinee is staying at the designated place under the quarantine order) from the personal data protection perspective for the Government's reference.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

In April 2020, the PCPD published its guidance regarding the health monitoring of incoming travellers and returning Hong Kong residents as follows:

- Authorities as data users or controllers should first seek to process the personal data in an anonymised or de-identified way;
- The least privacy intrusive measures should be adopted;
- Purpose Specification Principle and the Use Limitation Principle must be complied with when collecting and using personal data;
- The monitoring measures shall be no more than necessary and be proportionate to achieving the pressing and legitimate purpose of combating the COVID-19 pandemic;
- All practicable steps must be taken to protect the personal data, especially health data, from unauthorised or accidental access, processing, erasure, loss or use;
- The monitoring measures shall be time-bound and only continue for as long as necessary to combat the COVID-19 pandemic; and
- Personal data must not be kept longer than is necessary for fulfilling the purpose of collection.

Link to the guidance:
https://www.pcpd.org.hk/english/news_events/media_enquiry/enquiry_20200415b.html

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Incoming travellers and returning Hong Kong residents who are allowed to undergo quarantine at home have to wear electronic wristbands and use the "StayHomeSafe" app. Privacy-friendly designs were incorporated into the app. For example, the app does not track the physical location of the users. Instead, the app uses "geo-fencing" technology to ascertain whether the users are staying at home by analysing the environmental communication signals at the users' homes, such as Bluetooth, Wi-Fi and other signals. If the users leave their homes, the signals will change and the app will notify the health authority. However, the signals cannot be used to reveal or track the physical locations of the users.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Scanning of QR code before entering a premises or getting on a taxi to record the visit.

What best describes the approach used to build the contact tracing app?
Other decentralised approach.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name:
"LeaveHomeSafe" app

Description:
The app allows users to record their visits to premises by scanning the QR codes displayed at the entrances of the premises. The visit records are stored in the users' smartphones. Only when a user is diagnosed with COVID-19, his/her visit records will be required to upload (with the user's consent) for the health authority to conduct epidemiological investigations. The app will also automatically download the anonymised visit records of infected persons to users' smartphones for matching with the users' own visit records. Users will receive COVID-19 exposure notifications if they have visited the same premises that an infected person has visited at about the same time.

Link to website:
https://www.leavehomesafe.gov.hk/en/

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced

Link to relevant legislation (if applicable):
G.N. (E.) 419 of 2021: https://www.gld.gov.hk/egazette/pdf/202125182e/egn202125182419.pdf

Details:
Under the directions of the Secretary for Food and Health made on 7 July 2021 pursuant to sections 4 and 6 of the Prevention and Control of Disease (Requirements and Directions) (Business and Premises) Regulation (Chapter 599F, Laws of Hong Kong) (namely, G.N. (E.) 419 of 2021), certain types of premises (such as bars, pubs and other catering businesses under certain modes of operation) are required to ensure that their customers have scanned the QR codes at the entrances of the premises using the 'LeaveHomeSafe' app before entering the premises in order to facilitate epidemiological investigation.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
Not disclosed.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Purpose specification: The purpose for which personal data will be used should be made clear to the data subjects (e.g. contact tracing and epidemiological investigation).

Data minimisation: Only minimum amount of necessary personal data should be collected for fulfilling the specified purpose.

Transparency: The policies and practices in relation to the processing of personal data should be disclosed to the public.

Accuracy: Personal data shall be accurate and up to date.

Use limitation: Personal data shall only be used for the original purpose of collection.

Data security: Personal data shall be protected against unauthorised or accidental access, processing, erasure, loss or use.

Retention limitation: Personal data shall not be kept longer than is necessary for fulfilling the purpose of collection.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The PCPD has provided advice to the Government on the protection of personal data privacy in the implementation of the "LeaveHomeSafe" app.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The PCPD issued a media statement on 19 February 2021 confirming that the 'LeaveHomeSafe' app is in compliance with the relevant requirements under the Personal Data (Privacy) Ordinance (Chapter 486, Laws of Hong Kong) for the following reasons. They are considered as good privacy practices in contact tracing:

- The "LeaveHomeSafe" does not have a location tracking function. Neither does it collect users' GPS data. Therefore, the app does not have the function of tracking users' movements.
- The downloading of the app, which can be used immediately after download, does not involve

registration of the users' personal data. No collection of any personal data is involved during the process of download.
- Visit records are kept on users' smartphones only, not in any Government systems. There is no transfer of personal data to the Government's system or operators of premises for retention.
- Visit records will be automatically erased after 31 days.
- Only in the unfortunate event of a confirmed infection as ascertained by the health authority will the infected person be required under the Prevention and Control of Disease (Disclosure of Information) Regulation (Chapter 599D, Laws of Hong Kong) to upload the relevant visit records and provide his/her name and contact telephone number to assist the health authority in contact tracing.

Link to the media statement:
https://www.pcpd.org.hk/english/news_events/media_statements/press_20210219.html

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Measures adopted in Hong Kong to address or mitigate the privacy risks associated with the development and use of the contact tracing app:

- Conducting privacy impact assessment and other risk assessment prior to rolling out of the app, and regular audit and reassessment thereafter;
- Minimising the collection and retention of personal data:
  - No registration is required before use;
  - No collection of GPS data; and
  - Minimum access rights to users' smartphones;
- A decentralised approach to data storage with visit records stored in users' smartphones;
- Storing visit records in users' smartphones in encrypted form;
- Disclosing the privacy policy on the app's dedicated website and in the app;
- Issuing press releases to disclose significant updates of the app; and
- Automatic erasure of visits records after 31 days.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Video conferencing software and various e-learning platforms, including the 'Hong Kong Education City' website found by the Government.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

DPIA is not expressly required for under the Personal Data (Privacy) Ordinance. However, the PCPD advised data users to conduct privacy impact assessment before the launch of any new business initiative or project that might have significant impact on personal data privacy.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Excessive collection of personal data: E-learning tools may tend to collect excessive amount of personal data in order to profile the users or for other purposes. Children may not be able to assess what kinds of personal data are unnecessary for using the e-learning tools, or to give meaningful consent to the collection and use of their personal data.

Sharing of personal data with third parties: Children's personal data may be shared with third parties (such as advertisers) for gains.

Data security: E-learning tools may contain security vulnerabilities that can be exploited by hackers. Inadequate security measures adopted by the users (e.g. using weak passwords) will further increase the data security risks.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Purpose specification: The purpose for which personal data will be used should be made clear to the data subjects (e.g. to provide online education to users).

Data minimisation: Only minimum amount of necessary personal data should be collected for fulfilling the specified purpose.

Transparency: The policies and practices in relation to the processing of personal data should be disclosed to the public.

Use limitation: Personal data shall only be used for the original purpose of collection.

Data security: Personal data shall be protected against unauthorised or accidental access, processing, erasure, loss or use.

Retention limitation: Personal data shall not be kept longer than is necessary for fulfilling the purpose of collection.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The PCPD issued the "Guidelines on Children's Privacy during the Pandemic" in April 2020, which provides practical guidelines for schools and parents. The guidelines include:

- Review the privacy policies and security measures of e-learning tools;
- Consider whether there are other less privacy-intrusive means to achieve the same purpose;
- Minimise collection of personal data by service providers;
- Disable online tracking and recording functions of the e-learning tools;
- If recording/tracking is necessary, explicitly inform parents and students in advance;
- Handle minors' personal data with extra care, even with prescribed consent from adults; and
- Ensure that teaching staff knows how to use these tools correctly, securely and in a privacy-friendly manner, and how to deal with incidents of loss of devices or stolen accounts.

Link to the guidelines:
https://www.pcpd.org.hk/english/news_events/media_statements/press_20200402.html

The PCPD also issued the "Guidance on the Use of Video Conferencing Software" in November 2020, which is applicable to teachers and students. Practical advice provided in the Guidance includes:

- Safeguard user accounts by setting up strong passwords, changing the passwords regularly, and activating multi-factor authentication;
- Ensure that the video conferencing software is up to date and the latest security patches have been installed;
- Use secure Internet connection for conducting video conferencing;
- Set up a unique meeting ID and a strong, unique password for each video conference; and
- Avoid discussing personal or sensitive information during a video conference as far as practicable.

Link to the Guidance:
https://www.pcpd.org.hk/english/resources_centre/publications/files/gn_wfh_video.pdf

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

The PCPD issued the guidance mentioned in section 5.6 above to raise the awareness of protecting personal data privacy in the use of e-learning tools.

Furthermore, as teenagers tend to spend more time on online learning and social networking during the pandemic, the PCPD issued a media statement in November 2020, urging teenagers to exercise greater vigilance when they go online. Advice provided to teenagers includes:

- Avoid indiscriminately disclosing personal data or photos online, including those of their family members;
- Turn off the cameras and microphones of their computers/electronic devices when they are not in use;
- Be careful when making friends online. Do not be too ready to trust new online friends;
- Beware of fraudulent websites, suspicious emails and hyperlinks, and false information in order to avoid thefts of personal data;
- If a website or email looks suspicious, do not click the web links or download documents or apps. Seek help from parents or teachers immediately;
- If there is any suspicion of naked chat fraudulent activities, report the matter to the Police immediately; and
- If personal data and/or photos are found improperly disclosed on internet, contact the relevant social media platforms to request removal of the personal data and photos; or contact the PCPD for assistance.

Link to the media statement:
https://www.pcpd.org.hk/english/news_events/media_statements/press_20201123.html

Italy - Garante per la protezione dei dati personali (GPDP)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: ‘*EU* Digital COVID Certificate’/‘EU Green Pass’ provided by Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021
Main purpose(s):
Used in all EU Member to facilitate free movement inside the EU. It will not be a pre-condition to free movement. When travelling, the EU Digital COVID Certificate holder should in principle be exempted from free movement restrictions: Member States should refrain from imposing additional travel restrictions on the holders of an EU Digital COVID Certificate, unless they are necessary and proportionate to safeguard public health. Recital 48 of by Regulation (EU) 2021/953 provides that Member States may process personal data for other purposes, if the legal basis for the processing of such data for other purposes, including the related retention periods, is provided for in national law, which must comply with Union data protection law and the principles of effectiveness, necessity and proportionality, and should contain provisions clearly identifying the scope and extent of the processing, the specific purpose involved, the categories of entity that can verify the certificate as well as the relevant safeguards to prevent discrimination and abuse, taking into account the risks to the rights and freedoms of data subjects.
Description:
Digital and/or paper format proof - valid in all EU countries - that a person has either a) been vaccinated against COVID-19; b) received a negative test result or c) recovered from COVID-19. Both will have a QR code that contains the information included in the certificates, as well as a digital signature to make sure the certificate is authentic. The information included in the certificates are also shown in human-readable form and provided in at least the official language or languages of the issuing Member State and English.
Link to website: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en#how-will-citizens-get-the-certificate and https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953

For domestic activities
Name: ‘Digital Green Certificates’(DGC), or ‘Green Passes’
Main purpose(s):
Introduced by the ‘Italy Reopens’ decree in accordance with the European Commission Proposal on the ‘EU Digital COVID Certificate’/‘EU Green Pass’ to enable travelling between Italian regions (orange and red areas of the country) and participating in public or sports events; enable access of family members and visitors, to hospitality and long-term care facilities, nursing homes (RSA), hospices, rehabilitation facilities and residential facilities for the elderly; in yellow areas of the country, it is required to join civil or religious functions. From the 1st of July the DGC will be valid as the ‘EU digital COVID certificate’

pursuant to Regulation (EU) 2021/953. In the final part of the year 2021, the use of the DGC has been progressively extended to other domestic activities by subsequent decree laws (decree No 105 of July 2021, No 111 of August 2021 and No 127 of September 2021). Indeed, from the 6th of August 2021 the DGC is mandatory to enable access to restaurants indoors, cinemas, theatres and concert halls; museums and exhibitions; swimming pools, gyms, and wellness centres; congresses and conferences as well as public competitions. From the 1st of September 2021, it is mandatory for all school and university personnel to access the workplace as well as for students to access the university. Failure to comply with this obligation is considered unjustified absence and from the fifth day of absence any type of remuneration is suspended. From the 1st of September 2021 the DGC is also mandatory to enable the use of public transports such as airplanes, trains, boats and busses. Also, these Lastly, from the 15th of October 2021, it is mandatory to access the workplace for all personnel of public administrations and private entities. If those personnel do not hold the DGP at the time of accessing the workplace they are considered unjustified absent and for the days of unjustified absence no remuneration is due. However, this will not have any disciplinary consequences or affect the right to their post. Moreover, all the said provisions do not apply to subjects excluded by age from the vaccination campaign and to subjects exempt from being vaccinated on the basis of suitable medical certification. In addition, other methods of checking the validity the DGP have been introduced but the safeguards remain unchanged (only data subject's name, date of birth, the unique identifier and the actual validity of the certificate are disclosed)

Description:
Digital and/or paper format document certifying whether the individual recovered from, was vaccinated against, or tested negative for Covid-19. It is issued and released through the national DGC platform and verified through the 'VerificaC19' app which aims at ensuring the current validity of a green pass; the green pass contains a QR Code allowing the verification of its authenticity and validity: checks based on this app, trough the scan of the barcode, will only disclose the data subject's name, date of birth and the certificate's unique identifier without displaying any other information contained in the green pass – i.e., whether the individual recovered from, was vaccinated against, or tested negative for Covid-19.
Link to website:
https://www.dgc.gov.it/web/

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary (travellers who do not hold a Digital COVID Certificate Member States are required to comply with other obligations such as self-isolation, health monitoring and testing).

For domestic activities
Mandatory.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 3 (provisions of national law extending the use of the DGP to other domestic activities and especially those making the DGP mandatory to access the workplace have been questioned by the public)

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved:
The EU Digital COVID Certificate contains name, date of birth, date of issuance, relevant information about vaccine/ test/recovery and a unique identifier. This data remains on the certificate and is not stored or retained when the validity and authenticity of a certificate is verified in another Member State.

Parties having access to the data:
Competent authorities of the Member State of destination or transit, or cross-border passenger transport services operators (such as airlines, trains, coaches and ferries) required by national law to implement certain public health measures during the COVID-19 pandemic.

For domestic activities
Personal data involved:
The same data as those contained in EU Digital COVID Certificate. Unlike other EU countries, national checks based on the 'VerificaC19' app, trough the scan of the barcode, only disclose the data subject's name, date of birth, the unique identifier and the actual validity of the certificate without displaying any other information contained in the green pass – i.e., whether the individual recovered from, was vaccinated against, or tested negative for Covid-19. The paper format shows only the QR Code on the "cover" along with name, date of birth and a unique identifier so as to keep the other data confidential.
Parties having access to the data:
Public officials, operators in charge of controlling entertainment activities; owners of accommodation facilities and public businesses, places and premises, with certified entry; air, sea and land carriers; health and social assistance facilities.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details:
A centralised storage is adopted for the purpose of issuing and verifying and accepting green certificates by competent health authorities (e.g. a hospital, a test centre, a health authority). Once issued, green certificates are stored on user's device. The personal data accessed during the verification process are not to be retained by the entities authorised to verify the validity and authenticity. This data remains on the certificate and is not stored or retained when a certificate is verified in another Member State.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:

- use of the DGC for domestic activities of everyday life or linked to certain manifestations of fundamental rights and freedoms or for purposes not adequately specified by national or law or even for purposes other than those set out in national or EU law (as well as possible adoption of local initiatives mandating the use of a green pass for additional, non-coincident purposes) raise concerns with regard to the principle of proportionality and might have significant impacts on the exercise of those rights and freedom by individuals leading to discrimination, for example between people residing in the various territories of the country;
- use of the DGC without any limitations suitable to minimize the possible negative impacts on the rights and freedoms of individuals as well as the risks of any kind of discrimination, for example, against those who, for clinical reasons or other reasons, may be unable to undergo vaccination;
- access, processing and storage of medical data not necessary for the envisaged purposes or use of verifying tools not ensuring data minimisation when the validity and authenticity of a certificate is verified;
- data inaccurate and not updated with possible exclusion of concerned individuals from certain benefits or discrimination against them resulting from the improper issuing or not issuing of the DGC;
- exercise of data subjects' rights, especially access and rectification, in time not compatible with the

short period of validity of the certificates contained in the DGC and immediacy of its uses
- lack of transparency with regard to the processing of personal data contained in the DGC and of users' awareness about improper handling of the certificate (for instance disclosure of uploading of QR code trough/on social media platforms)
- breaches of confidentiality by intermediaries (health professionals), involved in the process of issuing and recovery of DGC;
- risks deriving from the components used to perform some inherent features of the DGC, such as the interaction with the 'Immuni' contact tracing App and IO App;
- storage periods not proportionate to the different period of validity of the certificates contained in the DGC (vaccine/ test/recovery)
- more in general, unauthorized access and or unlawful processing; unauthorized or accidental disclosure also due to possible improper behaviors of users, according to their degree of awareness in the use of digital technologies; unauthorized or accidental modification; accidental or unlawful loss, destruction; temporary or prolonged unavailability of the data.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.

Details:
With regard to the 'EU Green Pass', by 31 March 2022, the Commission shall submit a report to the European Parliament and to the Council on of the impact of the Regulation (EU) 2021/953 on the facilitation of free movement, fundamental rights and non-discrimination, as well as on the protection of personal data during the COVID-19 pandemic. The report may be accompanied by legislative proposals, in particular to extend the period of application of the Regulation, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.

Details:
Regulation (EU) 2021/953 on the 'EU Green Pass' shall apply from 1 July 2021 to 30 June 2022. The 'Digital Green Certificates'(DGC) is a public health measure justified to respond to the exceptional health situation of the Covid-19 pandemic and as such its duration is linked to the duration of the health emergency declared by national law.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

All Member States must provide digital solutions for the issuance of the EU Digital COVID Certificate, notably an app or portal for issuing both digital and paper certificates, a solution for citizens to store them (wallet app, existing tracing app) and a scanning solution for verification (with a smartphone using an app, for example). Moreover, each issuing body at national level (e.g. a hospital, a test centre, a health authority) has its own digital signature key. All of these are stored in a centralized database in each country. The European Commission has built a gateway connecting national databases that contain public signature keys. Through EU gateway all certificate signatures included in the QR codes of the certificates can be verified across the EU. The personal data of the certificate holder does not pass through the gateway, as this is not necessary to verify the digital signature. The European Commission also helped Member States to develop national software and apps to issue, store and verify certificates and supported them in the necessary tests to on-board the gateway. The technical specifications were agreed by Member States on 21 April in the eHealth network (a voluntary network connecting national authorities of EU Member States responsible for

eHealth pursuant to Article 14 of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare)

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

- lawfulness and purpose limitation (the purposes for which producing a green pass may be required should be laid down clearly by way of primary legislation);
- proportionality (the use of DGC should be limited only those events that are most at risk because of the large number of people present, excluding in principle places that relate to the daily activities of the population and those related to certain usual manifestations of fundamental freedoms; further uses may be justified only for reasons of substantial public interest if they are provided national law, in compliance with the EU legislation on data protection and the principles of effectiveness, necessity and proportionality and suitable and specific measures are in place to prevent discrimination and abuse, taking into account the risks to the rights and freedoms of the data subjects; therefore the law should set out among others: a minimum threshold of simultaneous attendance, beyond which the possibility of requesting the green pass is authorized; the reasons of substantial public interest, on the basis of the law, which may justify the use of the green pass for activities that involve access to places where daily activities take place or those related to the exercise of fundamental rights and freedoms; the scope of the processing, the purposes, the categories of subjects who can verify the certificate; suitable and specific guarantees to prevent any kind of discrimination and abuse, for example, against those who, for clinical reasons, or other reasons may be unable to undergo vaccination);
- data minimization (the draft decree of the Prime Minister's Office implementing the 'Italy Reopens' decree with regard to the National DGC Platform provides that the certificates include the minimum amount of personal and medical data that are necessary for the envisaged purposes - the same as those contained in EU Digital COVID Certificate-; moreover, the green pass may only be verified through a tool ensuring that the access of the authorised persons is limited to the data subject's identity and validity of the certificate without displaying any other information contained in the green pass – i.e., whether the individual recovered from, was vaccinated against, or tested negative for Covid-19; lastly personal and medical data during the verification process are not to be retained);
- suitable and specific guarantees, in terms of data protection, should be implemented with regard to subjects who are exempted from the obligation to hold and display the DGP (possible certifications to be issued to those persons in compliance with the principle of minimization must not involve the disclosure of unnecessary personal data and, in particular, health data);
- identification of categories of persons in charge of verifying the DGC who may have access to the data and responsible for uploading the data in the DGC Platform (a close list is provided in the same draft decree);
- transparency (other than the information provided in compliance with Article 13 and 14 of the GDPR, initiatives at national level should be put in place with a view of informing data subjects about sensitivity of the data contained in the DGC, emphasizing that they are required to disclose those data to persons in charge of the controls required by law)
- to ensure accuracy and updating of data the exercise of the right of rectification by data subjects pursuant to Article 16 of the GDPR through a telecommunication service of public utility ensuring a reply within a reasonable period of time taking into the period of validity of the certificates contained in the DGC
- integrity and confidentiality (the draft decree enlists several technical and organizational measures to be adopted to ensure the confidentiality, integrity and availability of the data processed, specifying the methods of access and use of the services, the components of the security infrastructure, the authentication process of authorized personnel, the logging of accesses and operations carried out, the retention periods, the security measures for the physical infrastructure and communication channels, the service monitoring system, the log analysis system, the measures against cyber-attacks, disaster recovery and backup).

With specific regard to the the EU Digital COVID Certificate provided by Regulation (EU) 2021/953 it should be highlighted that:
These certificates will only include the minimum amount of information that is necessary. This data cannot be retained by visited countries. For verification purposes, only the validity and authenticity of the certificate is checked, by verifying who issued and signed it. During this process, no personal data is exchanged. All health data remains with the Member State that issued an EU Digital COVID Certificate. The EU Digital COVID Certificate system will not require the setting up and maintenance of a database of health certificates at EU level, and no personal data will be exchanged via the EU gateway.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

The President of the Italian SA provided preliminary indications the constitutional aspects of the possible introduction of a "vaccination passport" for citizens who have received the anti SARS-COV2 vaccine in a hearing at the Parliament held on n 8 April 2021 (available in Italian at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9574242)

The Italian SA (Garante per la protezione dei dati personali) issued a warning to all the Ministries involved and other stakeholders, on 23 April 2021, pursuant to Article 58, paragraph 2, lett. a), of the GDPR, with regard to the processing of personal data carried out in relation to the 'Digital Green Certificates'(DGC) for Covid-19 provided for by the 'Italy Reopens' decree (Legislative Decree No 52/2021). The warning was also sent to the Prime Minister's office with a view to the relevant follow-up. On this occasion, the Italian SA highlighted the criticalities of the current text of the decree: in particular, it reminded the Government of the need for the law due to be enacted following the above decree to spell out the cases in which an individual would be required to produce a green pass in order to access certain premises or places. Moreover, the Garante pointed out that the major criticalities it has found could have been addressed beforehand expeditiously if the drafters of the decree had initiated the required dialogue with the SA pursuant to EU and Italian laws and had thus requested the necessary opinion from the SA without postponing such in-depth assessment. (see Decisions No 156 of 23 April 2021 available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9578184).

The President of the Italian SA provided further indications on issues related to the Covid-19 green certificate in another hearing at the Parliament held on 6 May 2021 (available in Italian at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9583365)

Indeed, the lack of clear-cut guidance on the conditions for producing a green pass has led a few regions and provinces in Italy to issue local orders mandating the use of a green pass for domestic purposes other than those set out in the 'Italy Reopens' decree. In this context, the Italian SA issued a warning to the Campania Region on 25 May 2021 pursuant to Article 58, paragraph 2, lett. a), of the GDPR, with regard to the processing of personal data related to the use of Covid-19 green certificates as additional preconditions to enable free movement and to access basic services including tourism, hotelling, wedding, transportation and entertainment-related ones (see Decision No 207 of 25 May 2021 available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9590466 and the English version of the press release at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9590434).

A definitive limitation of the processing was imposed, pursuant to Article 58, paragraph 2, lett. f), of the GDPR to the Autonomous Province of Bolzano with regard to the processing of personal data related to Covid-19 green certificates for uses different from those identified by the 'Italy Reopens' decree and in manner inconsistent with the provisions of the draft implementing decree of the President of the Council of Ministers on which the Garante issued a favourable opinion on 9 June 2021 (for more details, see below). In particular, according to the provincial orders issued by the President of the Autonomous Province of Bolzano the display of those certificates was required as a pre-condition to access places and activities such as restaurants indoors, accommodation facilities, training courses, theatres, concert halls, cinemas, conferences and congresses, museums and places of culture, as well as to carry out activities related to the workplace and to access healthcare services (see Decision No 244 of 18 June 2021 available at

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9671917).

Another warning was issued to the Sicilian Region pursuant to Article 58, paragraph 2, lett. a), of the GDPR with regard to the processing of personal data relating to the vaccination status of personnel of public administrations and regional bodies, entailing restrictions on individual rights and freedoms that could only be introduced by a national statutory law. Indeed, the regional order provided that all employees in direct contact with the public were "formally invited" to get the vaccination and, in the absence of this, moved to another job, thus introducing a requirement for the performance of certain tasks on a regional basis, which entails an unequal treatment with respect to personnel performing the same tasks throughout the country (see Decision No 273 of 22 July 2021 available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9683814).

Thereafter, following several fruitful exchanges with the Ministry of Health, the Italian SA issued a favourable opinion on the whole of the Prime Minister's draft decree which implemented the 'Italy Reopens' decree with regard to the National DGC Platform for the release of digital green certificates and laid down adequate safeguards for the use of such certificates (see Opinion No 229 of 9 June 2021 available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9668064 and the English version of the press release at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9668146). With this opinion, the Italian SA also assessed the DPIA provided by the Ministry of Health on the processing of personal data through the National DGC Platform. Indeed, the draft decree took on board most of the recommendations and guidance provided by the Garante during the exchanges with the Ministry of Health. However, there remained a few areas for which amendments were needed in the Italian SA's view. In particular, it requested that the purposes for which producing a green pass may be required should be laid down clearly by way of primary legislation. Such legislation has to provide that a green pass may only be issued and released through the national DGC platform and verified only through the 'VerificaC19' app. The latter app is the only tool that can ensure that checks on the current validity of the certificate based on this app only disclose the data subject's name, date of birth and unique identifier without displaying any other information contained in the green pass – i.e., whether the individual recovered from, was vaccinated against, or tested negative for Covid-19. A further measure to be implemented following the requests made by the Italian SA to the Ministry of Health envisages that only dedicated, trained staff will have to be deployed for checking green passes. As for obtaining a green pass, the draft decree envisages the use of various digital tools – including the website of the national DGC platform, the personal e-health file, the 'Immuni' app, and the 'IO' app (all of them will enable data subjects to access, display and download the respective certificates, but data subjects will also be able to apply to their family doctors or to pharmacies in order to download their green passes). Regarding, in particular, the apps for obtaining one's green pass, the Italian SA authorised the national digital contact tracing app 'Immuni' app but did not give its green light to the IO app, for the time being, on account of the criticalities that were found. More specifically, the company, which manages payment transactions involving public bodies, in charge of the development and management of the IO app, was ordered to provisionally limit certain data processing activities as performed via the app since they entail interactions with services by Google and Mixpanel and result accordingly into transfers to third countries of highly sensitive data without adequately informing users and enabling them to give their consent (see Decision No 230 of 9 June 2021 available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9668051). After the Italian SA stepped in, the company developed several technical measures to protect the privacy of users of the IO app which were implemented in a new version of the app. Taking account of the new measures taken, the Italian SA decided that the limitation of processing order it had issued could be lifted and expressed a favourable opinion on the use of the IO app for the purposes of obtaining the digital 'green passes' (see Decision No. 243 of 17 June 2021 available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670670).

With regard to the decree law which, from the 1st of September 202, extended the use of the DGC to access the workplace for all school and university personnel, the Italian SA issued its favourable opinion on the Prime Minister's draft decree which introduced simplified procedures for checking the Covid-19 green certificates of school personnel, alternatives to the ordinary ones providing for the use of the 'VerificaC19' app, which can still be used. In particular, educational institutions, as employers, will limit themselves to

verifying - through the Education Information System and the National DGC Platform - the mere holding of the Covid-19 green certificates by the staff, processing only the necessary data and in a manner that would avoid discriminatory effects, even indirect ones, in the workplace (see Decision No. 306 of 31 August 2021 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9694010).With regard to the 'EU Green Pass', the European Data Protection Board and the European Data Protection Supervisor adopted a joint opinion on the Commission's Proposals for a Digital Green Certificate. With this Joint Opinion, the EDPB and the EDPS invited the co-legislators to ensure that the Digital Green Certificate is fully in line with EU personal data protection legislation. They highlighted the need to mitigate the risks to fundamental rights of EU citizens and residents that may result from issuing the Digital Green Certificate, including its possible unintended secondary uses. In particular, the EDPB and the EDPS underlined that the use of the Digital Green Certificate may not, in any way, result in direct or indirect discrimination of individuals, and must be fully in line with the fundamental principles of necessity, proportionality and effectiveness. Moreover, given the nature of the measures put forward by the Proposal, the EDPB and the EDPS considered that the introduction of the Digital Green Certificate should be accompanied by a comprehensive legal framework (the Joint Opinion is available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_en)

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

See the previous answer.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

- Transparency requirements in the development and use of health passports or similar measures (see the previous answers)
- Minimisation of the collection and retention of personal data (see the previous answers)
- Use and disclosure limitation, preventing misuse for further incompatible purposes (see the previous answers)
- Data security measures and measures to prevent data in the 'health passports' or similar measure(s) from being tampered with (see the previous answers)
- Ethical concerns, such as the risk to discrimination and the right to liberty of movement (see in this regard the document adopted by the Italian Committee for Bioethics entitled "Passport, license, green pass in the context of the Covid-19 pandemic: bioethical aspects" on 30 April 2021, which has been taken into account by the Italian SA in Opinion No 229 of 9 June 2021, available at http://bioetica.governo.it/media/4226/p141_2021_passaporto-patentino-green-pass-nell-ambito-della-pandemia-covid-19-aspetti-bioetici_itdocx.pdf);
- Efficacy and effectiveness of the 'health passports' or similar measures (see the previous answers)
- Interoperability of the 'health passports' with those in other jurisdictions (from the 1st of July the DGC will be valid as the 'EU digital COVID certificate' pursuant to Regulation (EU) 2021/953)

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine

- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities
- Others: Covid-19 vaccination, certification of recovery or DGC for EU countries; reporting entry into the national territory to public health authorities; attestation provided to the carrier indicating foreign countries and territories in which the person stayed or transited in the 14 days prior to entering Italy and reasons for moving, as well as, depending on the foreign country of origin or transit, full address of the home or residence in Italy; private means of transport used to reach that place; telephone number; undergoing health monitoring by public health authorities.

For all incoming travellers from abroad, it is also required to fill in the European Digital Locator Passenger Form (dPLF) that has also to be verified by the carrier upon boarding in order to facilitate contact tracing by public health authorities in case travellers are exposed to an infectious disease during their travel.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

- Lack of transparency with regard to processing activities;
- Data inaccuracy especially with regard to the provision of individuals attestations
- Access, collection and storage of unnecessary data
- Longer than necessary storage periods
- Non-selective or unauthorized access

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

- Transparency of processing activities;
- Data accuracy especially with regard to the provision of individuals attestations
- Data minimisation and storage limitation
- Selective access by only authorized personnel

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Collaboration with the Ministry of Health and other public health authorities.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No, it has not.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Purposes, condition and methods of health monitoring provided by law, regulations and administrative instructions; information provided to data subjects in compliance with the GDPR; storage limitation periods; identification of authorized personnel.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: 'Immuni' App
Description:
When users discover they have tested positive for the virus, the app allows them to anonymously alert people they have been in close contact with and who may also have been infected. The alert includes advice on how to deal with the situation. To determine that a contact has taken place between two users, Immuni uses Bluetooth Low Energy technology and does not use geolocation data of any kind, including GPS data. In particular, the app emits a Bluetooth signal that includes a random code on a continuous basis. The codes do not contain any information about the user or their device and also change several times every hour. By doing so, the app can determine a contact without knowing who those users are and where they met. Indeed, Immuni doesn't collect any data that would identify the user, such as their name, date of birth, address, telephone number, or email address (no signing up procedure is requested to users). If a user is tested positive for the virus, with the help of the healthcare worker who notified him/her of his/her positive test result, he/she is able to report this result to the app, sharing his/her random codes and alerting the people he/she has been in close contact with. For every user, the app regularly downloads the random codes shared by users who have tested positive for the virus. By doing so, it can check if any of these codes correspond with those recorded in previous days. It will check the length and the distance of the contact to evaluate the risk of infection, and, if necessary, it will notify the persons concerned by the risky contacts. The data is used solely with the aim of containing the COVID-19 epidemic or after being made anonymous for public health, prophylaxis, statistical or scientific research purposes and they are saved on servers in Italy and managed by public bodies. The data controller is the Ministry of Health.
Link to website: https://www.immuni.italia.it

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.
Link to relevant legislation:
https://www.gazzettaufficiale.it/eli/id/2020/06/29/20A03469/sg
Details:
Article 6, Decree Law No 28 of 30 April 2020 and subsequent amendments and addenda, provides that:

- Immuni is functional only to the purpose of public health of containing the COVID-19 epidemic;
- the download of the app is voluntary;
- further processing of the collected data is excluded except the possibility of using it in anonymous and aggregated form for other purposes public health, prophylaxis, statistical or scientific research in compliance with Articles 5, paragraph 1, let. a) and 9, paragraph 2, lett. i) and j) of the GDPR;
- the controller of the data processing is the Ministry of Health pursuant to Article 28 of the GDPR;
- the app is rolled out after the carrying out of a DPIA by the Ministry of Health, the consultation and

authorization of the data protection authority that may prescribe measures safeguarding the data subjects' rights and interests pursuant to Article 36, paragraph 5, of the GDPR;

- by design according to Article 25 of the GDPR, data collected are exclusively those necessary to alert users they have been in close contact with other users confirmed positive for COVID-19, as well as to facilitate medical assistance vis-à-vis those persons;
- before activating the application, users receive clear and transparent information, pursuant to Article 13 and 14 of the GDPR, in order to achieve full awareness of, among others, the purposes and processing operations, the pseudonymisation measures and data retention periods;
- only proximity data of devices are collected, excluding the use of geolocation data of any kind, including GPS data;
- data confidentiality is ensured as well as the integrity, availability and resilience of systems and appropriate measures to avoid the risk of re-identification (in particular the data saved on the individual's smartphone and the connections between the app and the server are encrypted);
- the data retention period is limited to the time strictly necessary for the pursuit of the indicated purpose and the data are deleted automatically at the expiry of the retention period;
- after an DPIA pursuant to Article 35 of the GDPR interoperability with platforms operating, with the same purposes, in the territory of the EU is allowed.
- the use of the application and processing of personal data are discontinued at the date of termination of protective and preventive health needs related to the spread of COVID-19, including across borders, identified by decree of Prime Minister, on proposal of the Ministry of Health, and in any case not later than December 31, 2021 and by same date all personal data processed must be deleted or made anonymous.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.
Major privacy risks:

- individuals' movements are tracked or become traceable;
- prejudicial consequences, disadvantages or discrimination in the exercise of individuals' rights and freedoms for people refusing to download the app;
- further processing of data collected for incompatible purposes;
- collection of geolocation data and identification of users (for instance if the random codes that smartphones exchange via Bluetooth contain information about the individual's device);
- collection of unnecessary data of users or of their device;
- lack of transparency with regard to the users not only about the functioning of the app but also about the possibility that the app generates alerts that do not always reflect actual risk conditions;
- not limited data retention;
- non-selective or unauthorized access; unlawful processing; unauthorized or accidental disclosure; unauthorized or accidental modification; accidental or unlawful loss, destruction; temporary or prolonged unavailability of the data.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

- lawfulness and purpose limitation;
- further processing only for compatible purposes;
- voluntary use of the system, resulting from a free choice of the individual (not constrained on the basis of possible prejudicial consequences, disadvantages or discrimination in case of refusal);
- identification of the bodies involved in the processing and definition of their role with regard to the processing;
- data minimization;
- carrying out of a DPIA prior to the rolling out of the app since the processing activities are likely to

result in a high risk to the rights and freedoms of individuals;
- clear and transparent information to the user in order to achieve full awareness of, among others, the purposes and processing operations, the risk of re-identification and the data retention periods;
- data confidentiality integrity and availability, as well as appropriate measures to avoid the risk of re-identification;
- limited retention periods and automatic erasure of the data at the expiry of the retention period;
- temporary nature of the measure.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The President of the Italian SA provided preliminary indications on the use of new technologies and the Internet to counter the Covid-19 epidemiological emergency in a hearing at the Parliament held on 8 April 2020. The Italian SA issued an Opinion on the draft statutory provisions introducing the measure on 29 April 2020. On the 1st June 2020, the Garante authorized the processing of personal data related to the COVID-19 alert system via the 'Immuni' app on the basis of the DPIA performed by the Ministry of Health. On the same date, the SA issued an Opinion on a draft decree of the Ministry of Economy and Finance relating to the processing of personal data carried out through TS System in the context of the COVID-19 alert system, which complemented the identification of personal data collected by the Immuni app - necessary to alert users they have been in close contact with other users who were confirmed positive for Covid-19- provided by the Ministry of Health and specified in the said DPIA. Afterwards, the so-called 'Ristori' Decree Law introduced a national telephone support service for people tested positive for Sars-CoV-2 virus who have had close contacts with persons tested positive or have received an alert through the contact tracing app. On 17 December 2020, the Italian SA issued an Opinion on a draft ordinance concerning the operating procedure of the aforementioned service. On 25 February 2021, the Italian SA issued another Authorization for the processing of personal data related to the COVID-19 alert system via the 'Immuni' app on the basis of the updated DPIA performed by the Ministry of Health with a view to implementing the requirements requested by the Italian SA in the authorization issued on 1st June 2020, as well as the possibility for an individual, tested positive for Sars-CoV-2 virus after a molecular swab test, to allow the Immuni app to autonomously alert people with whom he/she have been in close contact, without the support of the healthcare professional (who communicated the positive result of the swab to the individual), or the support of the national telephone support service (so-called 'unlocking' of Immuni app directly by the patient). Therefore, on the same date the Italian SA issued another Opinion on a draft decree of the Ministry of Economy and Finance modifying the existing provisions on the processing of personal data carried out through TS System in the context of the COVID-19 alert system so as to implement the necessary functionalities to allow the "unlocking of the Immune app directly by the patient", from the mobile device on which the app is installed.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

President of the Italian SA, Hearing on the use of new technologies and the Internet to counter the Covid-19 epidemiological emergency held on 8 April 2020 at the Parliament (available in English at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9308774#english_version)

Italian SA, Opinion No 79 of 29 April 2020 available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9328050 on the draft provisions of statutory law introducing the Immuni app.

Italian SA, Authorization for the processing of personal related to the COVID-19 alert system via the 'Immuni' app on the basis of the DPIA performed by the Ministry of Health, Decision No 95 of 1st June 2020, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356568). Based on the impact assessment provided by the Ministry, the SA considered the processing of personal data within the framework of that system to be proportionate since measures have been put in place to adequately safeguard the rights and freedoms of data subjects by mitigating the risks possibly resulting from the processing. However, taking account of the complexity of the alert system and the number of individuals potentially involved, the

Garante considered it necessary anyhow to set out several measures in order to enhance security of the data related to the individuals downloading the app. Those measures will be implemented as part of the testing phase of the system so as to ensure that any residual criticalities are coped with prior to the full deployment phase. More specifically, the Garante requested users to be informed adequately about operation of the algorithm used to assess the exposure risk; users will have to be also made aware that the system might generate exposure alerts that do not entail in all cases an actual risk situation. Users will have to be enabled to temporarily deactivate the app through an easily accessible function on the home page. The data collected via the alert system may not be used for purposes other than those specified in the legislation regulating the app. Transparency of the data processing for statistical and epidemiological purposes will have to be ensured and appropriate safeguards for that processing will have to be laid down; to that end, any matching with identifiable individuals will have to be prevented and adequate security measures and anonymisation techniques must be in place. Any processing operations performed by system administrators on operating systems, the network and databases will have to be logged. The IP addresses of mobile phones will have to be stored for a period commensurate to what is strictly necessary to detect malfunctioning or attacks. Technical and organisational measures will have to be implemented to mitigate the risks related to false positives. Special care will have to be taken in drafting the information notices and alert messages, given that the system may also be used by minors aged above 14 years. Finally, the Garante has emphasized that processing by unauthorised entities of the personal data collected via the app may entail a criminal offence.

Italian SA, Opinion No 94 of the 1st June 2020 on a draft decree of the Ministry of Economy and Finance relating to the processing of personal data carried out through TS System in the COVID-19 alert system (available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9357932)
Italian SA, Opinion No 273 of 17 December 2020 the draft order of the Extraordinary Commissioner for the implementation of the measures necessary for the containment and contrast of the COVID-19 epidemiological emergency available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9516719).
Italian SA, Authorization for the processing of personal related to the COVID-19 alert system via the 'Immuni' app after the update of the data protection impact assessment carried out by the Ministry of Health, Decision No 65 of 25 February 2021 (available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9555987)
Italian SA, Opinion No 66 of 25 February 2021, on a draft decree of the Ministry of Economy and Finance modifying the existing provisions on the processing of personal data carried out through TS System in the context of the COVID-19 alert system with regard to implementation of the necessary functionalities to allow the "unlocking of the Immuni app directly by the patient" from his/her mobile device on which the app is installed (available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9561715)

See also the Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak adopted on 21 April 202 by the European Data Protection Board available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

- Conducting of data protection / privacy impact assessment and other risk assessment prior to rolling out the contact tracing app, and regular audit and reassessment thereafter
- Minimisation of the collection and retention of personal data
- A decentralised approach to data storage and processing
- Prohibiting against misuse of personal data for incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy)
- Efficacy and effectiveness of the contact tracing app
- Temporarily deactivation of the app through an easily accessible function

- Termination of the contact tracing app and erasure of data collected by the app
- Interoperability of the contact tracing app with similar apps in other jurisdictions

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Google Meet; G Suite; WeSchool; Google Classroom, etc.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

In selecting e-learning technologies, schools and universities have to take into account their specific features, including technical ones, preferring those which, both in the design phase and in the subsequent development, have such properties as to allow data controllers and data processors to fulfil their data protection obligations by design and by default (see Recital 78 and Article 25 of the GDPR). This choice, regarding the most appropriate technologies for distance learning, must also be made on the basis of the indications provided by the Data Protection Officer, who should be promptly involved in order to provide the necessary technical and legal support. Data protection impact assessment (DPIA), provided for by Article 35 and 36 of the GDPR for processing activities likely to result in a high risk to the rights and freedoms of individuals, is not necessary if the processing of personal data carried out by schools and universities, as regards minors and workers, does not present additional elements likely to increase those risks. For example, a DPIA is not required for the processing activities not performed on a large scale, such as, for instance, those carried out by a single school in the context of the use of an online videoconferencing service or a platform that does not allow the systematic monitoring of users and does not employ new invasive technological solutions (such as, among others, those involving geolocation or the collection of biometric data).

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

- in general, the role of external providers of e-leaning tools (on line services and/or digital platforms) with regard to the processing of personal data including the transfers of those data to third countries;
- making the use of e-learning services conditional upon the signing of a contract or the provision of consent to the processing of individuals' personal data for the provision of additional online services or further features by digital platforms, not necessary for educational purposes (e.g. geolocation or social login systems), especially where complex online platforms (providing services not aimed exclusively at teaching) are used;
- in setting up the accounts associated with children, students and/or teachers, the use of procedures for the identification and authentication of users which are not adequately robust;
- in case of audio-video recordings of lessons held, misuse or loss of control of the materials and video lessons made available by teachers on the digital platform, with possible prejudice to data protection rights and other rights (e.g. copyright). In particular, when those materials are subject to improper communication or dissemination (for example by publishing them on blogs or on social networks);
- the use of children's personal data for marketing or profiling purposes, taking advantage form the fact that they may be less aware of the risks, consequences and their rights;
- not transparent, intelligible and easily accessible information to children, students, parents and teachers regarding the essential characteristics of the processing activities carried out by the providers of e-

learning tools and digital platforms (especially when minors are involved and the information are provided in a language not easily understandable by them);

- specific risks arising from the use of the so-called proctoring, which consists in the use of remote monitoring systems aimed at identifying students attending tests/exams and checking the regularity of these tests (e.g. evaluating personal aspects relating to a person based solely on automated processing of personal data, including profiling, in particular, to analyze aspects concerning the behavior or reliability of data subjects; processing of biometric data and use of facial recognition technologies; data transfers to third countries)

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

- lawfulness (processing of children's or students' personal data by educational institutions is necessary for the performance of a task carried out in the public interest vested in the schools while parental consent cannot be considered a suitable legal basis since the activities carried out, albeit in a virtual environment, are activities institutionally assigned to educational institutions);
- the role and responsibilities of external providers of e-leaning tools for compliance with the obligations on the protection of personal data must be a governed by a contract or other legal act (in particular, educational institutions must ensure that suppliers of those tools provide sufficient guarantees to put in place technical and organizational measures appropriate to the specific processing activities performed on their behalf and that the data processed on their behalf are used only for e-learning purposes, without introducing additional purposes unrelated to educational activities)
- fairness and transparency (educational institutions must provide transparent, intelligible and easily accessible information to children, students, parents and teachers regarding the essential characteristics of the processing activities carried out on their behalf; in particular external providers of e-learning tools and digital platforms should be indicated, as well as the possible use of cloud technologies and data transfers to third countries)
- data minimization (it is necessary to verify that e-leaning services are configured in such a way as to minimize personal data to be processed both during the activation of the services and the use of them by teachers, students and children especially where complex platforms including a wider range of services, not aimed exclusively at teaching are used, avoiding for instance, the use of data on geolocation, or social login systems)
- storage limitation (educational institutions must ensure that the system chosen for the provision of e-learning services comply with the envisaged time limits for the data storage and subsequent erasure of data and they must therefore provide, in the act governing the relationship with external providers, specific instructions on data retention, deletion or return of data at the end of the provision of e-learning services, as well as on the handling of personal data breaches)
- implementation of the adequate safeguards in case of international transfers of personal data collected by e-learning tools;
- technical and organizational measures ensuring appropriate security of personal data (adequate procedures for the identification and authentication of users; robust processes for assigning users credentials or authentication devices; different authorization profiles for authorized subjects r to guarantee selective access to data; adequate password policies; storage of user passwords, through the use of state-of-the-art hashing functions and salt of adequate length; use of secure transmission channels taking into account the state of the art; measures to ensure data availability; perimeter protection systems; constantly updated anti-virus and anti-malware systems; periodic updating of basic software in order to prevent its vulnerability; logging of processing operations to verify lawfulness and fairness of data processing activities; user training and awareness).

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The Italian SA issued preliminary indications with regard to distance learning on 26th March 2020 (see Decision No. 64 of 26 March 2020 available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9300784)

In addition, the Italian SA developed and published in its website some FAQs concerning, more in general, the processing of personal data in schools in the context of the health emergency due to the pandemic based on the general guidance provided by it regarding complaints, alerts or queries. Some of them concerns the use of distance learning tools and video conference systems (available at https://www.garanteprivacy.it/temi/coronavirus/faq).

Furthermore, a working group was established between the Italian SA and the Ministry of Education dealing with the protection of personal data in the context of e-learning. Within the working group and in collaboration with the SA, the Ministry adopted and published on its website Guidelines on "Integrated digital education and privacy protection: general indications " (available at https://www.istruzione.it/rientriamoascuola/allegati/Didattica-Digitale-Integrata-e-tutela-della-privacy-Indicazioni-generali.pdf) as well as a number of FAQs on the "PROTECTION OF PERSONAL DATA" (Section No. 11) available at https://www.istruzione.it/rientriamoascuola/domandeerisposte.html)

Lastly, on 27th April 2021 the President of the Italian SA provided indication to the Parliament on the matter in a Memorandum on the "Impact of integrated digital teaching (DDI) on learning processes and on the psychophysical well-being of students" (available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9581498)

As for the proctoring, on 16 September 2021 the Italian DPA ordered to an University a limitation of the processing and imposed an administrative fine pursuant to the GDPR with regard to a series of infringements of data protection rules resulting from the use of a monitoring system for the remote performance of students' exams involving the processing of biometric data (available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9703988)

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

- Provision of guidance to schools, parents and students
- Assessment of privacy impact or risk assessment by schools
- Assessment of the necessity, effectiveness and proportionality of exam monitoring measures and tool
- Specific instructions on data retention, deletion or return of data at the end of the provision of e-learning services, as well as on the handling of personal data breaches in the contract or legal act governing the relationship between educational institutions and external providers
- Implementation of the appropriate data security measures in the e-learning tools
- Implementation of the adequate safeguards for cross-border transfer of personal data collected by e-learning tools
- Policies regarding the recording of audio and video of lessons

Japan - Personal Information Protection Commission (PPC)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Not yet, but it is being planned / considered by the government.

For domestic activities
Not yet, but it is being planned / considered by the government.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities
- Others:
    - Presenting a certification of inspection within 72 hours from the date of sample collection to the departure time of the flight.
    - Submission of a written pledge not to use public transportation for 14 days and to install a contact confirmation application, etc.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

NIL.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

NIL.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

NIL.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NIL.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

NIL.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: COVID-19 Contact-Confirming Application (COCOA)
Description:
The app, developed by the Ministry of Health, Labor and Welfare (MHLW), records the history of contacts of more than certain level between the apps users (so-called "close contact") by using Bluetooth of mobile terminals. The app notifies the users promptly in case where they were in a close contact with users tested positive for the COVID-19, so that they can take appropriate subsequent actions such as to receive instructions from a public health center. The app has been developed based on application programming interfaces (APIs) offered by Apple and Google.
When a user tested positive for COVID-19, he/she can register the Processing Number issued by a public health center in the app. The app then notifies other users who were in a close contact with him/her. It is not intended that the app complements manual contact tracing. The use of the app and the register of the Processing Number are on voluntary basis.
Link to website: https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00007.html

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
The app involves sensitive information, whether the users are tested positive or have been in a close contact with a person tested positive, and that could lead to an invasion of individuals' interest such as discriminations against certain users. Thus the administrator, etc. of the app should give due regard to their handling of the users' privacy information.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

The Experts' Meeting on Contact Tracing Apps, members of which consist of experts in the field of privacy, cyber security, IT as well as the health care workers, and the relevant government entities such as the PPC Japan and MHLW participated as observers, assessed the specifications of the app and put together the points to be noted into a report. The report pointed out that besides the obligation under the Act on the Protection of Personal Information Held by Administrative Organs and the Act on the Protection of Persona Information, since the app needs to gain trust of general public while it involves sensitive information whether the users are tested positive or have been in a close contact with someone tested positive, it should obtain the users' consent in principle at the crucial phases like starting the use and registering the positive test result, as well as give due regard to the privacy at each stage of the information life cycle (obtain, store, use, transfer and delete), regardless of the relevant provision of the said Acts. And, this point reflected into the specifications and the development of the app. Moreover, the report also mentioned the necessity of transparency, inclusiveness, limitation and verification of purpose, etc. as the points to be noted in administration of the app. The privacy policy of the app respects these points and it is publicly available.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The PPC Japan took part in the Experts' Meeting on Contact Tracing Apps as an observer. The Experts' Meeting drafted the specifications for the app and assessed its privacy and security aspects. The PPC Japan also published a statement expressing its views on effective use of contact tracing app to help deal with Coronavirus disease (COVID-19) before the Experts' Meeting established. The said statement explains PPC's view on how to utilize such apps with paying attention to the balance between the demands for securing the rights and the interests of individuals related to personal information and those for public policy use as a countermeasure against infectious diseases. The PPC's views were taken into account when drafting the specifications of the app, and reflected in the design of the app.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

As already mentioned in 3.7, the PPC Japan also published a statement expressing its views on effective use of contact tracing app to help deal with Coronavirus disease (COVID-19).

https://www.ppc.go.jp/en/legal/covid-19_2en/

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

- Concurrently with drafting the specifications of the app, the Experts' Meeting on Contact Tracing Apps made an assessment of the app on the aspects of protection of personal information and privacy. Furthermore, after the app was published, the Experts' Meeting assessed the app again on the new function added to the app, at the time of its implementation, in September 2020.
- The app does not collect information such as names, contact details (phone numbers etc.) and location information.
- The records of "close contact" are stored only within each user's mobile devise, and will not be sent out to the third party nor stored at the central server.
- The privacy policy of the app prohibits the use for purposes other than the original intent.
- The source code of the app is publicly available.
- The use of the app is based on the user's consent, and the consent can be revoked at any time. All stored information will be irrecoverably deleted by deleting the app from mobile device.
- Information of close contact is deleted automatically after 14 days.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

NIL.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Regardless of the sector, PPC works on the promotion of PIA conducted by private companies, and PPC has just published a report about points to be noted on conducts of PIA.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

NIL.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

NIL.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NIL.

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**
NIL.

Liechtenstein - Data Protection Authority

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: EU/EWR Digital COVID Zertifikat
Main purpose(s): The COVID-Certificate serves as an easy, secure and verifiable proof of a Covid-19 vaccination, of an undergone infection, and of a negative test result. The certificate is being adopted in the EEA at the same time as in the EU. Its purpose is to ensure that national confirmations are being accepted throughout Europe. Liechtenstein developed its own “EU/EWR Digital COVID Zertifikat”. Each certificate is provided with a unique QR-code, which serves as a base for any control.
Description:
The “EU Digital COVID Zertifikat” encompasses 3 certificates:

- vaccination-certificate
- recovery-certificate
- test-certificate

For each of these certificates an own QR-code is being generated for verification.

Main features of the certificates are:

- digital version on a mobile device
- printable version on paper
- QR-code with central information and a digital hallmark
- free of costs
- in national language (German) or English
- safe and secure environment
- valid in all EU/EEA-countries and Switzerland

Precondition for display of the digital «EU Digital Covid Zertifikat» is the digital identity (eID.li) and the respective mobile application which can be registered for free of costs. Alternatively, the “EU Digital COVID Zertifikat” can be carried as paper (hard copy) with a QR-code on it.
Link to website: https://www.serviceportal.li/de/privatpersonen/gesundheit-vorsorge-und-pflege/coronavirus/covid-zertifikat?pimcore_preview=true&_dc=1624429358076

For domestic activities
Name: EU/EWR Digital COVID Zertifikat
Main purpose(s): (see above)

Description: (see above)
Link to website: https://www.serviceportal.li/de/privatpersonen/gesundheit-vorsorge-und-pflege/coronavirus/covid-zertifikat?pimcore_preview=true&_dc=1624429358076

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Mandatory for proof of vaccination, recovery or second negative test result (see also below section 2.1)..

For domestic activities
Mandatory only for certain domestic activities (e.g. visits of interior areas of restaurants, bars, etc.).

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 3

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: Name, Surname, date of birth, date of issue, relevant information on vaccination/tests/recovery, unique identifier.
Parties having access to the data:

- Health department
- Controllers of the certificate (visible: name, surname, date of birth, status of the certificate (ok / not ok))

For domestic activities
Personal data involved: Name, Surname, Date of Birth, Date of issue, relevant information on vaccination/tests/recovery, unique identifier.
Parties having access to the data:

- Health department
- Controllers of the certificate (visible: name, surname, date of birth, status of the certificate (ok / not ok))

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Both centralised storage and decentralised storage on users' devices are adopted.
Details:

- Health department (for a maximum of 12 months to issue the certificates)
- Users' devices (downloaded certificates)

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

No information available.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.

Details: The EU regulation (EU) 2021/953 regulating these certificates expires automatically on 30 June 2022. If the pandemic lasts longer, an active prolongation or a new regulation would be necessary.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

- EU/EEA-regulation for interoperability of all such certificates throughout EU/EEA-countries. Data transfers in the same countries are regulated by the common data protection regulation GDPR.
- Close legal and technical cooperation as well with Swiss authorities to secure interoperability also with Swiss certification system. (Data transfers to Switzerland are covered by an adequacy decision of the EU Commission.)

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Art. 5 GDPR.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

The DPA stands ready for advice in data protection issues. So far, this has not been requested by the health department.
The DPA could also conduct controls or investigate complaints if any.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

- Transparency requirements in the development and use of health passports or similar measure(s)
- Minimisation of the collection and retention of personal data
- Use and disclosure limitation, preventing misuse for further incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Measures to prevent data in the 'health passports' or similar measure(s) from being tampered with
- Adequate safeguards for cross-border data transfers
- Ethical concerns, such as the risk to discrimination and the right to liberty of movement
- Efficacy and effectiveness of the 'health passports' or similar measure(s)
- Interoperability of the 'health passports' with those in other jurisdictions

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory entry form for every person
- In addition:
  - Health passport (COVID-Certificate) for persons vaccinated or recovered persons
  - Proof of negative test result for COVID-19 for persons not vaccinated and not recovered on entry and again 4-7 days after arrival (COVID-Certificate)
  - Proof of vaccination when arriving from certain countries/regions considered to have a high risk for an infection

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Violation of data protection principles of Art. 5 GDPR.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Art. 5 GDPR.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

The DPA stands ready for advice in data protection issues.
The DPA could also conduct controls or investigate complaints if any.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

No information available.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: SwissCovid App
Description: In Liechtenstein the Swiss contact tracing app can be used. For more information on it, please see the website below which is also available in English.
Link to website:
https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, existing legislation was amended.

Link to relevant legislation: https://www.fedlex.admin.ch/eli/cc/2015/297/de

Details: The Liechtenstein government has declared applicable also in Liechtenstein relevant parts of this Swiss legislation on the fight against epidemics.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Liechtenstein has not conducted an own DPIA for the SwissCovid App.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Art. 5 GDPR.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The DPA has evaluated several providers and their contact tracing apps for the health department and issued according (non-)recommendations.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

- Conducting of data protection / privacy impact assessment and other risk assessment prior to rolling out the contact tracing app, and regular audit and reassessment thereafter
- Minimisation of the collection and retention of personal data
- A decentralised approach to data storage and processing
- Prohibiting against misuse of personal data for incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy)
- Efficacy and effectiveness of the contact tracing app
- Termination of the contact tracing app and erasure of data collected by the app
- Interoperability of the contact tracing app with similar apps in other jurisdictions

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Swiss E-learning platforms; Apps such as Book Creator, Explain Edu, Anton, Garage Band etc.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Yes.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Violation of data protection principles of Art. 5 GDPR; in particular transparency, data retention and transfer of data to third states such as the US

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Art. 5 GDPR.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No. However, the DPA has issued several decisions regarding non-compliance of schools with data protection requirements in this regard.

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

- Assessment of privacy impact or risk assessment by schools
- Assessment of the necessity, effectiveness and proportionality of exam monitoring measures and tools
- Implementation of the appropriate data security measures in the e-learning tools
- Implementation of the adequate safeguards for cross-border transfer of personal data collected by e-learning tools
- Policies regarding the recording of audio and video of lessons
- Provision of guidance to parents

Lithuania - State Data Protection Inspectorate

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: EU Digital Green Certificate
Main purpose(s): to facilitate safe and free movement during the COVID-19 pandemic within the EU.
Description: it is a proof that a person has been vaccinated against COVID-19, has received a negative test result or has recovered from COVID-19 that can be used across all EU Member States. When travelling, the EU Digital COVID Certificate holder should in principle be exempted from free movement restrictions: Member States should refrain from imposing additional travel restrictions on the holders of an EU Digital COVID Certificate, unless they are necessary and proportionate to safeguard public health.
Link to website: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

For domestic activities
Name: National certificate (in Lithuania: galimybių pasas)
Description: It was also meant to be used for other restricted activities, e. g. catering (indoor), accommodation services, fitness clubs and pools, meeting convicts in detention (in contact), etc., but after these restrictions are annulled, currently, with the National Certificate people are able to participate in indoor and outdoor events with unlimited number of spectators.
Link to website: https://gpasas.lt/?lang=en

1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

For domestic activities
Voluntary.

Details (if applicable): in general data subjects are free to choose whether to use this national certificate or not, as data subjects are able to access the services (in most cases) by alternative means, for example to have a lunch outside (no certificate required). But if data subjects want to use restricted services, e. g. go to a concert, where unlimited amount of people are present physically, the national certification is mandatory.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5):
EU Digital Green Certificate: 4
National certificate: 3

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: The EU Digital COVID Certificate will only contain necessary information such as name, date of birth, the certificate issuer and a unique identifier of the certificate. In addition:

- For a vaccination certificate: vaccine type and manufacturer, number of doses received, date of vaccination;
- For a test certificate: type of test, date and time of test, place and result;
- For a recovery certificate: date of positive test result, validity period.

Parties having access to the data: The EU Digital COVID Certificate system will not require the setting up and maintenance of a database of health certificates at EU level, and no personal data will be exchanged via the EU gateway.

For domestic activities
Personal data involved:
To generate the National Certificate, the following personal data of special categories are processed: diagnosis that a person has recovered from COVID-19 disease; records about testing: COVID-19 test performed; testing or test result; date and time of sampling; data on vaccination: name of the vaccine, date of vaccination; vaccine dose according to the vaccination schedule (first, second).

To issue the National Certificate, the following data are processed (visually displayed on a device): 1) general data - name, surname and year of birth; 2) special data of the National Certificate: the beginning and expiry date of validity of the National Certificate and time, and QR code, which encodes data subject's general data, the beginning date of validity and expiry of the National Certificate and time, or information that contact activities are limited.

To verify the National Certificate, the following data are processed: QR code, which encodes data subject's general data and information about the starting date of validity and expiry of the National Certificate and time

Parties having access to the data:

- Police Department under the Ministry of the Interior of the Republic of Lithuania (to determine the person's compliance with the criteria of Resolution);
- the officer who controls the implementation of quarantine measures or the service provider as well as to other natural persons or legal entities who make decisions on the use of less restrictive quarantine measures in cases specified in Point 2.2 of the Resolution;

More information on data processing:
https://eimin.lrv.lt/uploads/eimin/documents/files/GP_Privacy_policy.pdf

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

Details: Existing data (eHealth) basis (where all data on vaccination, diseases and etc. is processed) is used for issuing the certificates.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

NIL.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

No.

Details: As for the National certificates, data controllers have the obligation to revise all the data processing operations that are carried out in their work, so such review should be made. State Data Protection Inspectorate has no information whether specific deadlines are set in this regard.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.

Details:
The EU Digital COVID Certificate will apply while regulation that brought it into effect is valid. The Regulation will apply for 12 months as from 1 July 2021. The Commission will present a report to the European Parliament and the Council on the application of the Regulation three months before the end of application of the Regulation. Together with this report, the Commission could propose to extend the date of application of the Regulation, taking into account the evolution of the epidemiological situation on the pandemic.

National certificate is linked to Resolution imposing restrictions during pandemic therefore, when such resolution will be annulled, the national certificate should be annulled / terminated automatically.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

The cross-border data transfer is not meant to take place.
As to the EU Digital COVID Certificate you may find all technical specification here: https://ec.europa.eu/health/ehealth/covid-19_en (see section "Trust framework and detailed technical specifications" and "More information")

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Lawfulness, Data minimisation, purpose limitation, integrity and confidentiality, accountability.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

As for the EU Digital COVID Certificate, State Data Protection Inspectorate has provided its comments on the regulation. More detailed assessment was made by European Data Protection Board (State Data Protection Inspectorate of the Republic of Lithuania is a part of European Data Protection Board) and European data protection supervisor.

As for the national certificate, State Data Protection Inspectorate participated, as an independent expert, in a working party (governmental level) that was looking how to implement the initiative to have a similar measure to EU Digital COVID Certificate that could be used in other contact services. Its role was to provide guidance on the requirements and risks.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Official public guidance has not been provided.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

- Minimisation of the collection and retention of personal data
- Use and disclosure limitation, preventing misuse for further incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Interoperability of the 'health passports' with those in other jurisdictions
- Prohibiting against misuse of personal data for incompatible purposes

State Data Protection Inspectorate does not have information on all measures adopted.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

All persons, arriving to Lithuania by all means of transport, including by car, are obligated to register with the National Public Health Center not earlier than 48 hours before their arrival to Lithuania. If using air or sea transport, persons will be asked to show a proof of registration before the begining of their trip. Registration form can be found here: https://keleiviams.nvsc.lt/en/form

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

NIL.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Lawfulness, Data minimisation, purpose limitation, integrity and confidentiality, accountability.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Legal acts, that has imposed requirement on health monitoring of incoming traveller, were provided for the assessment (as required by law).

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Official public guidance has not been provided.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

State Data Protection Inspectorate does not have such information.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: “Korona Stop Lt”
Description: Phones that use the app register the Bluetooth signals from other nearby phones. If the signal is sufficiently close and long enough, an anonymous code referring to a close contact will be stored in their phone. If a person now confirms their infection with the Korona Stop LT app, the anonymous keys on their device will be uploaded to a central server where all users can download them. It is not possible to identify a person based on an anonymous code. The user’s phone compares whether the infected person’s anonymous code matches a code previously stored on their phone. If so, the user is considered to be a close contact and they will be notified. It will not be revealed to the user who the infected person was with whom they were in contact with, or any other information that would allow the indirect identification of the infected person. Downloading and using the app is entirely voluntary.
Link to website: https://koronastop.lrv.lt/en/korona-stop-lt-app

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

State Data Protection Inspectorate does not have that information.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Lawfulness, Data minimisation, purpose limitation, integrity and confidentiality, accountability.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Data controller has submitted State Data Protection Inspectorate amendments to the regulations of transmissible disease, including the ones in connection with processing of personal data in relation with an app, also amendment to the rules of self-isolation. State Data Protection Inspectorate has provided its comments to the legal acts that were to be adopted.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Official public guidance has not been provided.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

- Minimisation of the collection and retention of personal data
- Decentralised approach to data storage and processing
- Prohibiting against misuse of personal data for incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy)

State Data Protection Inspectorate of the Republic of Lithuania does not have information on all measures adopted.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

State Data Protection Inspectorate does not have information on all e-learning tools that have been used.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Such recommendation has not been provided by State Data Protection Inspectorate. DPIA is not necessary in all the cases, it all depends how the remote learning is to be organised. But data controller is obliged to make an assessment whether DPIA is necessary by themselves, taking into account requirements of Article 35 of GDPR and State Data Protection Inspectorate's list of mandatory DPIA cases (you may find it here).

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

The major risks are related with the scope of personal data processed and appropriate security measures. There are a lot of different tools available in the market and some of them are highly intrusive or they do not have an option to blur / change background behind the student (which may lead to discrimination or bullying later on). Some of the tools does not ensure the appropriate security of the data / communication (tool does not use appropriate protocols, stores data in third countries without appropriate implementation of Section V of GDPR, or does not allow to deleted the stored data when required and etc.). Also, ensuring of data subject rights is also quite vague in some tools. Therefore, it is very important to make a detailed assessment of tool to be used in remote learning so that all the risk would be mitigated.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Lawfulness, Data minimisation, purpose limitation, integrity and confidentiality, accountability.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes, State Data Protection Inspectorate published guidance on what elements should be assessed before starting remote learning:

1. Determining the roles and responsibilities of the staff of the educational institution;

This part explains elements that are important to consider determining the roles and responsibilities of the staff of the educational institution, e. g. a person who is responsible for security policy should be involved in the process of organisation of remote learning; informing students on how they can report the security incidents; informing of teachers and parents on their data processing (including cookies) and how to use remote learning tools (including their obligations related to the usage of these tools), etc.

2. Choosing the appropriate means of remote learning;

This part explains elements that are important for choosing a tool for remote learning, e. g. size of the group that would use it; type of remote learning (passive / active); age of the data subjects that would be using the tool (will they be keen to use it); whether remote learning tool can be used with authorised access only; does this tool stores logs; how / whether does the access control / data subjects rights are ensured; where and how long personal data are stored and etc.

3. Document the usage of remote learning tools

This part explains what elements should be included in the documentation on the usage of remote tool for emote leaning, e. g. roles and responsibilities of parties, who is entitled to provide / change / restrict / terminate the access to a tool; what personal data are necessary for usage of this tool; conditions and requirements for usage of selected tool (including for video sharing); how to control the attendance of students; etc.

Link to a guidance: Three steps for organisation of remote learning.

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

State Data Protection Inspectorate does not have such information.

Macao, China - Office for Personal Data Protection (GPDP)

個人資料保護辦公室
Gabinete para a Protecção de Dados Pessoais
Office for Personal Data Protection

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Not yet, but it is being planned / considered by the government.

For domestic activities
Yes.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For domestic activities
Name: The Health Code and Vaccination Record Scheme
Main purpose(s): to achieve herd immunity and to acknowledge individuals' access to specific facilities as well as to facilitate cross-border control
Description: Serving as a digital system for certifying the health condition of individuals
Link to website: https://app.ssm.gov.mo/healthPHD/page/index2.html

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For domestic activities
Voluntary.

Details (if applicable):
It functions to work as a self-declaration of having no symptoms, and denial of having exposure history or travel history

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 4

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For domestic activities
Personal data involved: name, gender, date of birth, ID number, contact numbers, address, health symptoms, travel and contact history as well as Nucleic Acid Test result and vaccination records

Parties having access to the data: Health Bureau

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.
No, decentralised storage on users' devices is adopted. Details: Personal data collected would be stored in the users' mobile devices and would help to generate coloured QR code accordingly. However, there is still a central data base held by the Health Bureau, with data uploaded/reported voluntarily by the data subject.
1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?
No, DPIA has not been conducted.
1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
No.
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
No.
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
Result of COVID-19 test and vaccination record would be shown along with the coloured QR code of users' mobile devices.
1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?
All measures being taken must always be aligned with the principles stipulated in the Personal Data Protection Act as well as other legislations such as the Law on Prevention and Control of Infectious Disease
1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?
Our office has kept itself open to giving necessary advices on the conformation of measures taken to combat the COVID-19.
1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
Yes. Currently it is not available for publication yet.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

NIL.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities
- Declaration of Travel and Contact History

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

NIL.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Principles of data minimisation, use limitation, data security and transparency are always be considered.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

The office takes the role to safeguard the privacy rights of all citizens.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

NIL.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Not yet, but it is being planned / considered by the government.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Voluntary QR code scanning.

What best describes the approach used to build the contact tracing app?
Other decentralised approach.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

NIL.

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

All principles stipulated in the Personal Data Protection Act should always be observed in the implementation of such type of measures.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The office takes the role to safeguard the personal data privacy rights by monitoring the proper use of sensitive data of individuals.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes. Not available for publication.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Nil.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, moderate increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Mobile learning through tablets and laptops as well as computer video-conferencing are widely used for student e-learning during the very early stage of the pandemic.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

NIL.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

The date security when using e-learning technologies did come into our concern.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

The same principles set forth in the Personal Data Protection Act apply.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The advices on the protection of students' personal data in the use of e-learning
20201027044227150.pdf (gpdp.gov.mo) (Chinese version only)

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

NIL.

Malta - Information and Data Protection Commissioner (IDPC)

1. ‘Health passports’
1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?
For cross-border/boundary travel Yes. *For domestic activities* Yes.
1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).
For cross-border/boundary travel Name: Vaccine Certificate Main purpose(s): For travel purposes Description: Maltese ID card holders to generate their Covid-19 Vaccine Certificate 14 days after getting fully vaccinated. Link to website: https://certifikatvaccin.gov.mt/ *For domestic activities* Name: Vaccine Certificate (the same as above) Main purpose(s): Also being used for domestic activities, such as entrance to visit elderly people homes. Description: Maltese ID card holders to generate their Covid-19 Vaccine Certificate 14 days after getting fully vaccinated. Link to website: https://certifikatvaccin.gov.mt/
1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.
For cross-border/boundary travel Voluntary. *For domestic activities* Voluntary.
1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?
Rating (on a scale of 1 – 5): 4

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: Name, surname, date of birth, disease or agent target, vaccination status, unique certificate issuer, passport or other identification document.
Parties having access to the data: Public health authorities of Malta and of a third country with whom Malta has a bilateral agreement.

For domestic activities
The same described above.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.
Details:
There is a database within the Superintendence of Public Health, in the case of the Vaccine certificate.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

Major privacy risks:
(No DPIA has been presented to this Office).
Green certificate is in accordance with the EU regulations
The Vaccine Certificate which has similar provisions.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

No.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.
Details: The policy is established by law (L.N. 203 of 2021 - Public Health Act cap. 465)

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

A vaccination certification is able to be verified in Malta and third country party by a bilateral agreement, based on a trust framework, by confirming the authenticity, validity and integrity.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Same principles according to the GDPR.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

Provided advice and involved in the drafting of the national law.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

Data minimisation, appropriate technical means based on trust framework which shall provide for appropriate technical and organisational measures to ensure adequate security to safeguard the confidentiality, integrity, availability and resilience of personal data being processed for such purpose.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities
- Others: Providing a vaccination certificate and / or EU green passport

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Security and data breaches.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

The same as those provided in the GDPR

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Advice in relation to data protection matters when arising.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Same as above.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Covid Alert Malta
Description: The COVID Alert Malta App is being provided by the Superintendent of Public Health and data is used solely for the purpose of exposure notification/contact tracing.
Link to website: https://covidalert.gov.mt/

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.

Link to relevant legislation: https://legislation.mt/eli/sl/465.52/eng
Details: This order shall apply to the processing of data by the Superintendent of Public Health by means of a contact tracing and alerting mobile application which supports contact tracing through theuse of proximity tracing technology and alerts users to take appropriate voluntary action, including testing or self-isolation, if potentially exposed to the COVID-19 virus.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
Data breaches and cybersecurity issues.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Same as the GDPR.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Review of DPIA, providing advice in the drafting of the legislation.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No guidance has been issued.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Same as above.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Team meetings technologies.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

The data controller should decide whether a DPIA is to be conducted.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Same as above.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?
Same as GDPR.
4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
No guidance has been issued.
4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**
Normal IT security measures. In addition, the education authorities together with state and privacy schools adopted policies in relation to recording of audio and video of lessons. Schools also communicate with parents of students.

Mauritius - Data Protection Office (DPO)

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: Policy at the level of Government to control arrivals at the airport managed by Ministry of Health and Wellness.
Main purpose(s): To minimise risks of the population being infected by COVID-19 and other communicable diseases.
Description: Declaration made by travellers for vacation or returning residents. Vaccination Card or PCR Test result requested.
Link to website: https://health.govmu.org/Pages/Main%20Page/Openingofborders.aspx
https://mauritiusnow.com/mauritius-travel-advice
https://mauritius-airport.atol.aero/passengers/covid-19-update

For domestic activities
Name: Access to School/University, visiting/accompanying family at public/private hospitals
Main purpose(s): To minimise risks of the population being infected by COVID-19 and other communicable diseases.
Description: Vaccination Card is required to access schools, public/private hospitals.
Citizens above 18 have to produce their vaccine card to get access to schools/universities/hospitals

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Mandatory.

For domestic activities
Mandatory

Details (if applicable): Section (4) of the COVID-19 (Restriction of Access to Specified Institutions) Regulations 2021 stipulates that for the purpose of preventing a spread of COVID-19 within Mauritius during the quarantine period, no person shall have access to a specified institution (including a kindergarten, a special education needs institution, a pre-primary school, a primary school, a secondary school, a tertiary institution, a vocational training centre and any other educational or training institution, whether Government-owned or private-owned) unless he produces -

1. his COVID-19 vaccination card certifying that he has been vaccinated with a COVID-19 vaccine; or
2. in case he has not been vaccinated with a COVID-19 vaccine, an RT-PCR test result slip certifying a negative result dating back to no more than 7 days from the date of the RT-PCT test was undertaken.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 3

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel

Personal data involved: Names, Date of Birth, Travel document No, Country of origin, Port of origin, close contact with covid-19 infected person, symptoms during the last 14 days) fever, cough, shortness of breath), Covid-19 test done during last 3 days, countries and cities visited during the last 14 days, date and signature.

Parties having access to the data: Ministry of Health and Wellness and the Data Processor (ATOL).

For domestic activities

Personal data involved: Personal Data on Vaccination Card namely:
Surname, Name, National ID/Passport No, Sex, Date of Birth, Age, Address, Tel No, Occupation, Next to Kin name, Next to Kin mobile number, Allergies, Name of Vaccine, Date of First dose, Date of second dose, Dosage, Time of injection

Parties having access to the data: Institutions (School, University, technical school, Ministry of Health) where it is mandatory to produce the vaccine card.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details: Yes, there is a central information system managed by the Ministry of health for all passengers arriving in Mauritius regarding PCR test. While for citizen of Mauritius, the vaccination card system is manual.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks: Please refer to answer in question 2.2

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.
Details: Managed by High level powered committee on Covid-19 and decisions taken at the Cabinet of Ministers level.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

No.
Details: In due course.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

Vaccination document or PCR test document have to be shown at the airport border control.
The Data Protection Act namely section 36 applies for transfers.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

The personal data are to be used for the purposes of controlling the spread of Covid-19 in Mauritius meeting the proportionality and necessity test.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

We provide advice regarding data protection issues and privacy.
We investigate breaches and conducts audits and checks.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes, we have issued a guide namely 'Guide on Data Protection for Health Data and Artificial Intelligence Solutions' which covers the processing of personal data in line with Data Protection Act 2017 during the Covid-19 pandemic.

1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**

- Transparency requirements in the development and use of health passports or similar measure(s)
- Minimisation of the collection and retention of personal data
- Use and disclosure limitation, preventing misuse for further incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Measures to prevent data in the 'health passports' or similar measure(s) from being tampered with
- Efficacy and effectiveness of the 'health passports' or similar measure(s)

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities
- Others: Recent PCR test results before travel in some cases.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

A DPIA was conducted by the Ministry of Health and Wellness regarding the screening and identifying all incoming passengers to Mauritius for communicable diseases more specifically COVID-19.

Major risk:

- Data being lost
- National Calamities/loss of data
- Unauthorised access or disclosure of personal data.

However, the following measures have taken to mitigate the risks:

- Secured data storage sites
- Controlled access with frequent change of passwords
- Offsite data backup
- A controlled access mechanism to restrict unauthorised personnel
- Audit trail facility
- Private key of SSL certificate
- Database hardening
- Validation and Captcha

Purpose limitation principle applied. The lawful basis is described in question 2.5 below.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Aggregate data are published on the number of people in quarantine, infected and released. Anonymisation applies.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

We assessed the Data Protection Impact Assessment and provide advice to the Ministry of Health and Wellness on this issue.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes.

We refer to section 28 (lawful processing), section 29 (special categories of personal data) and section 31 (security of processing) of the Data Protection Act 2017 in our advice as provided below.

In this context, section 28 which is on lawful processing and section 29 which is on special categories of personal data, will apply since the Ministry of Health and Wellness will be processing health data of individuals/patients. Hence, the Ministry of Health and Wellness can rely on the following exceptions to process the data:

a) Section 28 (1)(b)(iv) - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

b) Section 29 (d)(ii)- the processing is necessary for the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in subsection (2);

c) Note: Section 29(2) of the DPA stipulates that the personal data referred to in subsection (1) may be processed for the purposes referred to in subsection (1)(d)(ii) where the data are processed by or under the responsibility of a professional or other person subject to the obligation of professional secrecy under any enactment.

d) Section 29 (d)(iii) – the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject.

According to section 31 of DPA, the controller(Ministry of Health) shall implement appropriate security and organizational measures to secure the protection of the personal data. Section 31(2) describes in a general manner the measures that can be implemented to secure the personal data.

Amongst other security measures, you may consider the followings:

- Back up media should be securely protected and appropriate physical security is in place.
- Encryption may be used if personal data are transmitted on an information and communication medium if the data flows outside the organization.
- Please ensure appropriate access rights are given to officers using the system with varying levels of access rights. Six roles have been defined in the OpenElis software. Ensure that is being respected by the System Administrator of the application system.
- Fine-grained audit trail may also be implemented in the application if required.
- Employees are trained to use the application securely.
- General security awareness is provided to officers.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Personal details of infected person are not published.
Quarantine and treatment are provided by the Ministry of |Health and Wellness according the Regulations passed.

THE COVID-19 (MISCELLANEOUS PROVISIONS) Act 2020
https://www.mymauritius.travel/mauritius-travel-alerts
https://mauritius-airport.atol.aero/passengers/covid-19-update

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No. Contact tracing is done manually by Ministry of Health and Wellness by interviewing all covid-19 positive persons.

New legislations have been introduced to facilitate contact tracing:
58_THE PREVENTION AND MITIGATION OF INFECTIOUS DISEASE (CORONAVIRUS) REGULATIONS 2020

THE COVID-19 (MISCELLANEOUS PROVISIONS) Act 2020

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Zoom, Microsoft Team, Google Meet and programmes on the National TV.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Yes.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

- Unauthorised use of pictures/video of participants.
- Sharing of video to parents who cannot assist their children during the class session.
- The making of video compulsory during the class.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

- Consent of parent or guardian is required for children personal data processing under section 30(1) of the DPA.
- Education institutions have to identify their lawful grounds for the processing of students' data.
- The implementation of appropriate security and organisational measures.
- Devise online learning policy and notify all students/parents and make the terms of use clear to all.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes.

Advice tendered to educational institutions.

The educational institution needs to have an online privacy policy where all the rules are clearly communicated to staff, students or guardians of students and which are in compliance with the Data Protection Act 2017 (DPA).

You will need to ensure the following:-

- Check the wording of your online privacy policy to ensure it covers your intended use of the information and identifies the appropriate lawful basis you are relying on. A sample template is provided for you to adapt to your institution. (Template_PrivacyNotification for Online Meeting.docx)
- Include in your work policies and staff handbook your policy on the recording of video-conferences. In addition, ensure that have all staff who may conduct such meetings received training in how to carry out the meeting lawfully.
- Carry out a Data Protection Impact Assessment (DPIA) to demonstrate that that all potential risks have been considered and how those risks will be mitigated as a recommendation.
- Signpost your online privacy policy to participants in advance, and at the start of the meeting request their verbal consent to record the session
- Keep records of your decisions to record meetings so that you can demonstrate you are complying with the DPA.
- Where the criteria under section 28(1)(b) of the DPA does not apply then you will need the consent of the participants (or guardians of minor students) for processing of their personal data.
- Ensure that the online collaborative tool provides all security options for the host to protect the personal data of each participant in an online class. Therefore, the host should ensure that all the security settings are properly configured.
- Inform parent (legal guardian) how the school as the controller will process his/her child's personal data during distance learning and what rights he or she has.

You may use any available technology for communication with parents of students and/or teachers provided it is secure and ensures confidentiality.

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**
• Assessment of privacy impact or risk assessment by schools • Assessment of the necessity, effectiveness and proportionality of exam monitoring measures and tools • Implementation of the appropriate data security measures in the e-learning tools • Implementation of the adequate safeguards for cross-border transfer of personal data collected by e-learning tools • Policies regarding the recording of audio and video of lessons • Training to staff using online meeting tools

Mexico - The National Institute for Transparency, Access to Information and Personal Data Protection (INAI)

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
No.

For domestic activities
No.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Relevant requirements

- body temperature to health authorities
- Others: Use of face mask

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

NIL.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Is not applicable because the processing of personal data is minimum.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Administrative procedures regarding with the data protection law.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NIL.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Not applicable.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No.

3.2 Please select the relevant characteristics of the digital contact tracing app:

Not applicable.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Not applicable.

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Not applicable.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Not applicable.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The Ministry of Health of the Mexican government ("Secretaría de Salud") released the national app "COVID-19MX" INAI, conducted an analysis of the national app to identify that the processing carried out by the application was in compliance with the legal framework on personal data protection, and then held meetings with the Ministry of Health to inform them of the findings. The COVID-19 MX app is not a contact tracing app, but requests various data points such as age, gender, telephone number, predisposed or vulnerability group (diabetes, hypertension, etc.), Address (only State and municipality are mandatory).

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Not applicable.

3.9 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.**

Not applicable.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, moderate increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Web conference platforms.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Article 74 of General Law on Protection of Personal Data Held by Obligated Parties established that when the data controller intend to put into operation or modify public policies, or computational systems or platforms, electronic applications or any other technology which, in its opinion and in with this Law entail an intensive or relevant processing of personal data, it must conduct an Assessment of impact on the protection of personal data and submit it to the Institute or the Guarantor bodies, as applicable, which can issue non-binding specialized recommendations on the subject of personal data protection.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Theft, damage, copying, destruction or use in an unauthorised manner, for subsequent unlawful use for fraudulent activities, exposing the integrity of the data subjects.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Code of good practices to guide the online processing of personal data of girls, boys, and adolescents. The Code contains a set of fifteen rules are intended to protect minors so that they can explore, learn and play online, guaranteeing adequate protection of their personal data.
Available at:
https://home.inai.org.mx/wp-content/documentos/pdpdoctosguias/codigobuenaspracticasnna.pdf

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

The authority has developed a Code of good practices to guide the online processing of personal data and adolescents.

Mexico - Transparency Institute, Access to Public Information and Protection of Personal Data of the State of Mexico and Municipalities (Infoem)

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
No.

For domestic activities
No.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

No.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

- Cloud storage
- Email
- Classes by videoconferences
- Digital platforms for collaboration, student-teacher

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

No.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Content risks: Exposure of children and young people to unwanted and inappropriate content, such as sexual, pornographic and violent images, racist, discriminatory or hateful when there are invasions to the videoconference rooms where the classes are taught.
Contact risks: Spam.
Behavioral risks: Taking photos or videos can be distributed without consent.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Institutions in the State of Mexico must comply with the principles of the Law on Protection of Personal Data Held by Obliged Subjects of the State of Mexico and Municipalities.

- Quality: Those responsible will adopt the measures to keep the personal data in their possession accurate, complete, correct and updated, so as not to alter its veracity.
- Consent: The processing of personal data in the possession of the obliged subjects will have the consent of the owner prior to the processing, except for the exceptions provided for in this Law and other applicable legal provisions.
- Purpose: All processing of personal data carried out by the person in charge must be justified by specific, lawful, explicit and legitimate purposes, related to the attributions that the applicable regulations confer on them.
- Information: The person in charge will have the obligation to inform through the privacy notice in an express, precise and unequivocal way to the owners, the information that is collected from them and for what purposes, the existence and main characteristics of the treatment to which Your personal data will be submitted so that you can make informed decisions in this regard.
- Loyalty: The person in charge may not obtain, collect, collect, process, or transfer personal data, through deceptive, fraudulent, unfair or illegal means, privileging the protection of the privacy interests of the owner of the information.
- Legality: The processing of personal data by the person in charge must be subject to the powers or attributions that the applicable regulations confers on it.
- Proportionality: The person in charge should only process adequate, relevant and strictly necessary personal data for the purpose that justifies its treatment.
- Responsibility: Educational institutions will comply with the data protection principles established in the Law, and must adopt the necessary measures for its application. The foregoing when the data were processed by a manager or third party at the request of the obligated subject.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

NIL.

Newfoundland and Labrador, Canada - Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC NL)

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Not applicable - International travel would be under the jurisdiction of the Canadian government, not the provincial government.

For domestic activities
The provincial government is not using a "passport", however does require an application from all travellers; the form is available online at Travel Form (nlchi.nl.ca). As there are different isolation requirements for various scenarios, the form asks individuals to indicate if they are vaccinated or partially vaccinated and to attach proof of vaccination. Newfoundland and Labrador is in a travel bubble with three provinces in Atlantic Canada (Nova Scotia, Prince Edward Island and New Brunswick) and, while those travelers need to complete the form, they are not required to self-isolate upon arrival. Travelers from other Canadian provinces may be subject to self-isolation depending on their vaccination status and test results.

For residents of the province that require proof of vaccination, there is a portal where same can be downloaded (Online Vaccination Records - COVID-19 Vaccine (gov.nl.ca)). This vaccination record includes date, brand name of vaccination and lot number of vaccination.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For domestic activities
Name: Travel Form
Main purpose(s): To screen all travellers entering the province of Newfoundland and Labrador
Description:
The government has a five step process for travellers:

1. Complete the travel form discussed above within 72 hours of expected travel date. Once completed, individuals will be provided with a reference number that should be retained; fully vaccinated individuals can re-use this reference number, while unvaccinated or partially vaccinated individuals will need a new reference number each time they travel.

2. Travel with proper identification: Non-Newfoundland and Labrador residents need two pieces of government issued identification; one must be a photo ID card and one must include a home address. Residents of Newfoundland and Labrador must present a provincial drivers license or photo ID card with address of principal residence and one of a number of other pieces of identification, such as an MCP card or a bank statement with a current address. Other options and combinations of identifications are available for anyone without a driver's license or photo ID card.

3. Get tested, if required. This varies depending on the traveller's vaccination status and self—isolation arrangements.

4. Self-isolate if required. This varies depending on the traveller's vaccination status. Further, unvaccinated rotational workers and essential workers have a modified self-isolation and testing schedule.

5. Follow Public Health Guidelines during their stay

Link to website: Travelling to Newfoundland and Labrador - COVID-19 (gov.nl.ca)

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For domestic activities
Mandatory.

Details (if applicable): As Newfoundland is an island, visitors enter by boat or air and are screened upon arrival. While Labrador is part of mainland Canada, there are very few roads connecting the province with Quebec. It is therefore relatively easy to ensure travellers have completed the required documentation and screening prior to entry.

The restrictions are identified in Special Measures Orders made under the Public Health Protection and Promotion Act (SNL2018 CHAPTER P-37.3 - PUBLIC HEALTH PROTECTION AND PROMOTION ACT (assembly.nl.ca)). All Special Measures Orders are available online at Public Health Orders - COVID-19 (gov.nl.ca). The most recent SMO involving travel was dated July 1, 2021 and is available at Special-Measures-Order-Re-opening-Travel-July-1-2021-1.pdf (gov.nl.ca).

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): We do not have the data required to respond to this question.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For domestic activities
Personal data involved:

- First name, last name and middle initial(s);
- Phone Numbers;
- Email;
- Address (home);
- country where travel commenced;
- province/state where travel commenced;
- number of people travelling together;
- whether you are a resident of Atlantic Canada who has not travelled outside Canada in 14 days;
- Arrival type;
- Date of arrival;
- Date of Birth;
- whether the duration of travel is less than 48 hours;
- information regarding the location, type and occupants of your isolation location and the personal information of your isolation support person;
- vaccine information including: status (fully, partially with a test – which must be uploaded -, partially without a test, not vaccinated); country of administration; vaccine name, lot number, and date of vaccination for each dose received and an uploaded image of a vaccination certificate.

Parties having access to the data:

- Department of Health and Community Services (Intake Personnel, Follow-up Personnel, and Department staff tasked with verifying randomly selected Travel Forms to ensure complete and to verify vaccine status information provided).
- Newfoundland and Labrador Centre for Health Information for data analysis (e.g. total Application count, how many approved and denied etc.) with personal identifiers removed.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details: All travel declaration forms are submitted electronically using an electronic program developed by the Newfoundland and Labrador Centre for Health Information at the request of the Department of Health and Community Services.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
NOTE: the following risks are identified in the most recent PIA; earlier PIAs were conducted on the travel declaration system, with the scope of the most recent PIA focused on the additional of the vaccination status. Further, most risks had suggested mitigation activities.

Privacy Risk 1: Personal information in the Travel Form may be retained for longer than required leading to non-compliance with legislation and may increase the likelihood of unauthorized access.

Privacy Risk 2: Lack of documentation related to account provisioning, and de-provisioning, user validation, user roles and appropriate access may result in unauthorized access to personal information and/or privacy breach.

Privacy Risk 3: Lack of a documented auditing plan may lead to undetected unauthorized access to personal information.

Privacy Risk 4: Lack of Two Factor Authentication (2FA) for Users to access personal information over an internet connection may expose the information to unintended or malicious breaches.

Privacy Risk 5: Agreements and contracts between Follow-up Personnel and the Department have not been assessed to determine if appropriate privacy clauses and protections are contained therein. If this information is not included in these documents then inappropriate collection, use and disclosure of information may occur or users may not be aware of their obligations regarding their use of the Travel Form Application.

Privacy Risk 6: Over-collection of personal information outside of what is requested on initial declaration form(s).

Privacy Risk 7: Over-collection of information based on identified purpose.

Privacy Risk 8: (Also Operational Risk 1) The unauthorized collection of information which may include personal information or personal health information of someone other than the relevant individual; or potentially harmful, malicious or abusive content.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
Unknown. OIPC NL indicated that it would follow-up on the system at an appropriate future date. With the situation changing fairly rapidly, it is difficult to identify a reasonable expectation regarding system evaluation and follow-up.
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
Unknown. There may already be internal discussions between the Chief Medical Officer of Health and the Department of Health and Community Services of which OIPC NL is unaware.
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
This is a system specific to travellers entering Newfoundland and Labrador. Each provincial government will develop its own requirements. OIPC NL is unaware of any plans for future interoperability.
1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?
The PIA for the traveller declaration form examined all 10 of the CSA data privacy principles.
1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?
OIPC NL has a good relationship with both the Department of Health and Community Services and the Newfoundland and Labrador Centre for Health Information. We are regularly contacted about upcoming initiatives and are provided with courtesy copies of PIAs for review before initiatives go live. While not under our jurisdiction, the Privacy Commissioner of Canada has been involving the provincial oversight offices when reviewing COVID initiatives planned by the federal government.
1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
In May 2021, the federal, provincial and territorial commissioners issued a joint statement about vaccine passports, available online at Privacy and COVID-19 Vaccine Passports - Office of the Privacy Commissioner of Canada. We assume that the submission from the Privacy Commissioner of Canada's Office summarized the statement.
1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.
While OIPC NL has had informal discussions on this topic, there has been no basis for engagement as the provincial government has not signalled any firm plans to move in this direction.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

Requirements vary depending on where the traveller is coming from and their vaccination status (for example, some travellers must self-isolate for 14 days upon arrival, others do not). Complete details are available at Public Health Orders - COVID-19 (gov.nl.ca).

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Potential over collection of personal health information and issues around informed consent. If travellers must provide information to enter the province, is consent free and voluntary?

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

The PIA examined the 10 CSA privacy principles and commented on each.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

The Department of Health and Community Services leads the COVID efforts in the province; the Department is both a public body subject to the Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015) and a custodian under the Personal Health Information Act (PHIA). Both acts establish expectations regarding the collection, use and disclosure of personal information and personal health information, as well as reasonable safeguards for the information. OIPC NL has oversight of both Acts.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

See AFrameworkForTheGovernmentOfNewfoundlandAndLabradorToAssessPrivacy.pdf (oipc.nl.ca), adapted from guidance issued by the Privacy Commissioner of Canada.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

OIPC NL is only aware of follow-up on those travellers required to isolate upon arrival; this follow-up is done by staff of the Department of Health and Community Services.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: COVID Alert (Canadian app)
Description: OIPC NL assumes that a detailed description has been provided by the Office of the Privacy Commissioner of Canada.
Link to website:
Download COVID Alert: Canada's exposure notification app - Canada.ca

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks: OIPC NL received a copy of the COVID Alert PIA through the Office of the Privacy Commissioner of Canada; OIPC NL assumes their submission discussed the risks identified.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Not applicable.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Initially, the provincial government was working on a provincial app and consulted with our Office during development. Once it was decided to use the national COVID Alert app, this consultation ended and the focus shifted to the provincial use of the federal app.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

In May 2020, a joint statements on contact tracing was published by the federal, provincial and territorial commissioners, available online at
Supporting public health, building public trust: Privacy principles for contact tracing and similar apps - Office of the Privacy Commissioner of Canada.

As this was published by the Privacy Commissioner of Canada's Office, OIPC NL assumes that it is summarized in their submission.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Not applicable.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Nil.

4.2 What are the popular e-learning technologies used in your jurisdiction?

NOTE: While learning moved online several times, it is our understanding that existing technologies were leveraged. OIPC NL has not been involved in any new e-learning technologies.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Yes. While private colleges are outside the jurisdiction of OIPC NL, the provincial university and community college, as well as the two school boards and the Department of Education, are public bodies subject to the Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015). OIPC NL identifies a PIA as best practice for such initiatives.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Not applicable.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

The 10 CSA Privacy Principles.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
Not applicable.
4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**
Not applicable.

New Zealand - Office of the Privacy Commissioner (OPC)

1. ‘Health passports’
1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?
For cross-border/boundary travel Not yet, but proposals in this area are being considered by the Government. *For domestic activities* Currently no.
1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).
Not applicable.
1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.
Not applicable.
1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?
Rating (on a scale of 1 – 5): We have no data from which to give an accurate answer.
1.5 Please list out the personal data involved in the ‘health passport’ or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.
Because we do not have a health passport in operation, this is difficult to answer completely.
1.6 Is the data collected by the ‘health passport’ or similar measure(s) stored or processed in any central databases? Please elaborate.
Not applicable.
1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the ‘health passport’ or similar measure(s)? What are the major privacy risks identified in the DPIA?
Not applicable – we have not seen a DPIA yet because the health passport is currently in development.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
Not applicable.
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
Not applicable.
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
Not applicable.
1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?
We would expect that the 'privacy by design' principles are embedded in our local solution's development. We would also expect that the local solution is Privacy Act 2020 (and/or the Health Information Privacy Code 2020) compliant.
1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?
We expect that we will have a larger role to play as our local solution is developed through consultatory advice.
1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
We have not issued official guidance or advice. We have written a blog post about health passports however.
1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**
We cannot yet answer this question at this early stage.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Collection of health information – for example:
    - Reporting body temperature to health authorities
    - Testing for COVID-19
    - Reporting other COVID-19 symptoms to health authorities

Those in quarantine facilities run by the Government are visited by nurses daily for their temperature, blood oxygen levels, overall health and so forth. They must undergo COVID testing throughout their stay. They are asked whether they have had any issues breathing, whether they have coughed or sneezed at all, whether they have had a runny nose or an 'cold symptoms' such as tiredness and aches. Their names, contact details, and GP are also provided Government facility operators.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Vast amounts of health information are being collected to ensure that NZ is COVID free. With that will always come risks to do with secure storage and ensuring those with the correct authorisation to access this information are the only people who can, ensuring that staff are aware of their obligations to keep the information confidential and only disclosing it as necessary, and that people's personal information is not used beyond the purposes for which it is collected (unless legal exceptions apply).

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

The key data protection principles are contained in the Health Information Privacy Code 2020 / the Privacy Act 2020.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

We regulate all agencies collecting, using, storing, and disclosing personal information. We also assist in guiding agencies toward best practice. The Ministry of Health and other central Government agencies have consulted us frequently to this end.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

We work with the Ministry of Health on a consultatory basis.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

As above.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: NZ Covid App
Link to website:
https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-resources-and-tools/nz-covid-tracer-app

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.

Link to relevant legislation:
https://www.legislation.govt.nz/act/public/2020/0012/latest/LMS344177.html
Details:
Section 11(1)(a)(ix).

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, a DPIA has been conducted.

Major privacy risks:
Scope creep – while the tracer app is privacy enhancing and the Commissioner has publicly backed the NZ app, we must ensure that as the app develops overtime that it remains privacy protective. If there are changes that have implications for privacy, there must be a clear need/authority.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

- Only collecting what is necessary for the purposes of contact tracing
- Ensuring that information is only kept for as long as necessary
- Ensuring that people are aware of the implications of use of the tracer app for their privacy
- Ensuring that there is clear authority for disclosure of data

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

We reviewed the DPIA and supported privacy protective upgrades such as the Bluetooth upgrade (this added the Bluetooth functionality) and the removal of the requirement for people to register their personal details when downloading the app. We are consulted as iterations of the app are developed.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Not applicable.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

We have supported privacy enhancing developments to the app as a when they have occurred as mentioned above. We also work with the Ministry of Health as it develops new versions of the app to ensure that the updates do not negatively impact people's privacy.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, a moderate increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Different schools implemented different technologies.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

We would always recommend a PIA be undertaken, however, there is no statutory requirement.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Not applicable.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

It will be crucial that students' data is collected fairly. Part of this is ensuring that students are aware of what data of theirs is collected. Furthermore, their personal information should not be over-collected. Because students have a diminished ability to exercise choice, schools and responsible authorities should ensure that this is not exploited and that only that information which is necessary for the purpose of providing education is indeed collected.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
Not applicable.
4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**
Not applicable.

Philippines - National Privacy Commission (NPC)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Not yet, but it is being planned / considered by the government.

For domestic activities
Not yet, but it is being planned / considered by the government.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Reporting body temperature to health authorities
- Testing for COVID-19
- Reporting other COVID-19 symptoms to health authorities

Quarantine and testing requirements vary depending on place of origin and/or destination.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

- Unauthorized/unlawful disclosure of personal data
- Use of personal data for unauthorized purposes
- Over collection/ disproportionate collection of personal data

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

- Transparency
- Proportionality
- Legitimate purpose
- Security measures
- Retention

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

The National Privacy Commission coordinates with the Philippines COVID-19 Inter-Agency Task Force for the Management of Emerging Infectious Diseases Resolutions on COVID-19 related data privacy concerns.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No specific issuance on health monitoring of incoming travellers and returning nationals but there is a joint statement of the Department of Health (DOH) and National Privacy Commission (NPC) on Processing and Disclosure of COVID-19 Related Data which emphasizes the lawful processing of personal data, lawful disclosure, and government's legal obligation to protect the data privacy rights of these patients and ensure the confidentiality, integrity, and availability of their personal data.

https://www.privacy.gov.ph/2020/04/npc-phe-bulletin-no-11-joint-statement-of-the-department-of-health-doh-and-national-privacy-commission-npc-on-processing-and-disclosure-of-covid-19-related-data/

https://www.privacy.gov.ph/wp-content/uploads/2020/10/jmc2020-0002v1.pdf

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

- Privacy Notices
- Anonymization of personal data; Names and other unique identifiers shall NOT be released publicly or shared with entities not directly involved in the care of the patient, or entities unauthorized by law or other legal instruments to process such information, without the patient's consent. Violations of this provision shall be punishable by the penalties set under the Data Privacy Act.
- Only information relevant to contact tracing and health monitoring are collected
- The Department of Health (DOH) and other government agencies involved and/or contributing to the contact tracing shall form a memorandum of agreement on data sharing to ensure proper use and accountability of personal information being collected.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?

- Bluetooth technology
- Using data from mobile operators

What best describes the approach used to build the contact tracing app?

- Centralised approach
- Exposure Notification API built by Google and Apple

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: StaySafe
Description: https://www.staysafe.ph/
Link to website: https://www.staysafe.ph/

Note: There are other contact tracing applications being used in other local government units and certain establishments as well but StaySafe is the contact tracing app endorsed for mandatory use by the Philippines COVID-19 Inter-Agency Task Force for the Management of Emerging Infectious Diseases Resolutions.

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.
Link to relevant legislation:
https://www.officialgazette.gov.ph/downloads/2019/04apr/20190426-RA-11332-RRD.pdf

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:

- Over collection/ disproportionate collection of personal data relative to purpose
- Retention period of personal data collected

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

- Transparency
- Proportionality
- Legitimate purpose
- Security measures
- Retention

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The National Privacy Commission coordinates with the Philippines COVID-19 Inter-Agency Task Force for the Management of Emerging Infectious Diseases Resolutions on the implementation of the contact tracing app.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NPC PHE BULLETIN No. 8: On COVID-19 -related apps, digital tools and solutions in this time of pandemic outlined certain considerations on the use of digital technologies and the processing of personal data to enable health authorities contain the COVID-19 pandemic, in a manner that is effective and preserves and protects the data privacy rights of individuals.
https://www.privacy.gov.ph/2020/04/npc-phe-bulletin-no-8-on-covid-19-related-apps-digital-tools-and-solutions-in-this-time-of-pandemic/

3.9 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.**

- Conducting of data protection / privacy impact assessment and other risk assessment prior to rolling out the contact tracing app, and regular audit and reassessment thereafter
- Minimisation of the collection and retention of personal data
- Prohibiting against misuse of personal data for incompatible purposes
- Data security measures
- Privacy notice accessible thru app and website

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

- Learning management system (LMS)
- Online productivity platforms (OPP)
- Videoconferencing platforms
- Messaging applications
- Emails
- Cloud/online documents storage platforms

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

- Recommend DPIA

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

- Unauthorized/unlawful disclosure of personal data
- Use of personal data for unauthorized purposes
- Data privacy breaches such as hacked portals and databases, phishing, stolen laptops, system glitches and human error,

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

- Transparency
- Proportionality
- Legitimate purpose
- Security measures
- Retention

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points

and provide the link to the guidance or advice, if available.

The advisory on online learning, among other things, provide that:

- An announcement or posting involving personal data, such as grades and results of assignments, must be viewable only by its intended recipient/s.
- Downloading of personal data stored in the LMS or OPP should be kept to a minimum and/or limited to that which is necessary for online learning.
- Mechanisms must be in place so that submissions, such as assignments and projects, may be carried out in a safe and secure manner.
- Submissions via social media platforms are discouraged.
- Posting or sharing of personal data, such as photos and videos, on social media, must have a legitimate purpose and be done using authorized social media accounts of the school.
- Explicit consent of the student (or parent or legal guardian, in the case of minors) should be obtained before the conduct of online proctoring and the use of related tools or technologies.

https://www.privacy.gov.ph/2020/10/npc-phe-bulletin-no-16-privacy-dos-and-donts-for-online-learning-in-public-k-12-classes/

https://www.privacy.gov.ph/2021/02/npc-phe-bulletin-no-17-update-on-the-data-privacy-best-practices-in-online-learning/

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

- Downloading of personal data stored in the LMS or OPP should be kept to a minimum and/or limited to that which is necessary for online learning.
- Mechanisms must be in place so that submissions, such as assignments and projects, may be carried out in a safe and secure manner.
- Posting or sharing of personal data, such as photos and videos, on social media, must have a legitimate purpose and be done using authorized social media accounts of the school.
- Explicit consent of the student (or parent or legal guardian, in the case of minors) should be obtained before the conduct of online proctoring and the use of related tools or technologies.
- Limit use of supporting tools or technologies that they have not officially adopted, as there is no formal relationship between them and the developer of the tools.
- Dos and don'ts guide for parents or guardians, such as helping the child or ward check and customize privacy settings of the device or application for online learning and teaching them basic online security

Poland - Personal Data Protection Office (UODO)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.
EU Digital COVID Certificate will be used in Poland, which as of 1 July 2021 enters into application throughout the EU – in all EU Member States, including Poland; it is a European Commission’s solution and relevant information on the EU Digital COVID Certificate is available on the European Commission’s website: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: EU Digital COVID Certificate
Main purpose(s): Please, see the EC website quoted below.
Description: Please, see the EC website quoted below
Link to website: The relevant information on the EU Digital COVID Certificate is available on the European Commission’s website: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

For more information please visit the European Commission’s website quoted above.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?

Rating (on a scale of 1 – 5): 3

1.5 Please list out the personal data involved in the ‘health passport’ or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
These issues are specified by the provisions of the Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

Details: The EU Digital COVID Certificate system will not require the setting up and maintenance of a database of health certificates at EU level, and no personal data will be exchanged via the EU gateway. According to recital 10 of the Regulation 2021/953 - This Regulation does not provide a legal basis for setting up or maintaining a centralised database at Union level containing personal data.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

No, DPIA has not been conducted.

Major privacy risks:
In view of the urgency, the Commission did not carry out an impact assessment.
However, according to the recital 58 of the Regulation 2021/953: At the latest three months before the end of the period of application of this Regulation, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic, the Commission should submit a second report to the European Parliament and the Council, on the lessons learned from the application of this Regulation, including on its impact on the facilitation of free movement and on data protection.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.
Details: See point 1.7 above.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.
Details:
According to the Art. 10 of the Regulation 2021/953:
(2) After the end of period of the application of this Regulation, no further processing shall occur.
(4) The personal data processed for the purpose of issuing the certificates referred to in Article 3(1), including the issuance of a new certificate, shall not be retained by the issuer longer than is strictly necessary for its purpose and in no case longer than the period for which the certificates may be used to exercise the right to free movement.
(5) Any certificate revocation lists exchanged between Member States pursuant to Article 4(2) shall not be retained after the end of period of the application of this Regulation.

The Regulation 2021/953 shall apply from 1 July 2021 to 30 June 2022.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

Please, see the Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

The certificates will only include the minimum amount of information that is necessary. This cannot be retained by visited countries. For verification purposes, only the validity and authenticity of the certificate is checked, by verifying who issued and signed it. During this process, no personal data is exchanged. All health data remains with the Member State that issued an EU Digital COVID Certificate.

Please, see also EDPB-EDPS Joint Opinion 04/2021 on 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 https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_en

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

As the member of the European Data Protection Board (EDPB) the Personal Data Protection Office in Poland participated in the drafting and adopting of the EDPB-EDPS Joint Opinion 04/2021 on 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

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

There are no specific measures adopted in Polish jurisdiction in this regard.

As the member of the European Data Protection Board (EDPB) the Personal Data Protection Office in Poland participated in the drafting and adopting of the EDPB-EDPS Joint Opinion 04/2021 on 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.
Source: https://edpb.europa.eu/news/news/2021/eu-data-protection-authorities-adopt-joint-opinion-digital-green-certificate_en

1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**

NIL.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19
- Others:

Schengen

- Travelers are quarantined unless they present a negative test for COVID-19. The test will have to be performed no earlier than 48 hours before crossing the border.
- Test type: PCR or antigenic.
- The solution will cover all means of transport: collective and individual transport as well as crossing the border on foot.
- Travelers who have been quarantined in Poland will be able to perform a test within 48 hours of crossing the border, the negative result of which will release them from quarantine.
- These tests are not publicly funded.

Not Schengen

- Each traveller is placed in a 10-day quarantine.
- You will not be able to be released from quarantine on the basis of a test performed within 48 hours upon arrival in Poland. This possibility is allowed only after 7 days.

Attention!

People traveling from India, South Africa, Brazil, Great Britain and Northern Ireland cannot be released from quarantine on the basis of a test performed within 48 hours after returning to Poland. This possibility is allowed only after 7 days. The obligation to undergo quarantine is deemed to be fulfilled when the negative test result is entered by the medical diagnostic laboratory into the ICT system.

Important! People vaccinated against COVID-19 are released from quarantine. This applies to people who have been issued a certificate of vaccination with a vaccine that has been authorized in the European Union. Full vaccination in the European Union will be recognized 14 days after the end of the vaccination process.

Important! There is currently no air traffic ban. Source: https://www.gov.pl/web/koronawirus/informacje-dla-podrozujacych

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

The major privacy risks identified by the Personal Data Protection Office concern the lawfulness of personal data processing in terms of, among others, the legal basis for measuring temperature to prevent the spread of COVID-19, sharing data of quarantined persons or creating registers containing information about such persons.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Processing of such information should comply with the principles set out in Art. 5(1) and (2) of the GDPR. So the data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject,
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed,

- kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed,
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

The Personal Data Protection Office is not involved in any activities in this regard.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

The EDPB adopted the Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak. The measures allowing for safe reopening of borders, which are currently foreseen or implemented by Member States, include testing for COVID-19, the requirement of having certificates issued by health care employees and using any contact tracing application. Most measures entail the processing of personal data.
The EDPB recalls that the data protection legislation remains applicable and allows for an efficient response to the pandemic, while at the same time protecting fundamental rights and freedoms. The EDPB emphasizes that the processing of personal data must be necessary and proportionate, and
the protection of personal data must be ensured consistently throughout the European Economic Area. In the statement, the EDPB urges the Member States to take a common European approach when deciding which processing of personal data is necessary.
https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-processing-personal-data-context-reopening_en

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Others: In case of the ProteGO Safe application, Apple/Google framework is used, based on mixed approach (hybrid/mixed).

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: ProteGO Safe, now renamed for STOP COVID
Description: It is a contact tracing application that performs risk assessment tests and enables the keeping of a health journal. The application consists of two modules. The first one is a self-monitoring module. It allows to check on an ongoing basis whether we are in a risk group and if yes, in which kind. This solution is based on the guidelines of the World Health Organization (WHO). The second module is scanning user's surroundings and communicating in case of risk of contact with the virus.

The application is based on the Privacy-Preserving Contact Tracing protocol and geolocation data is not used for its operation. Ultimately, data from the application (an anonymous identifier of his device, which will allow to warn other users who had the application installed) are to be sent to health authorities only on the basis of explicit consent after prior contact from a representative of such authority.

Link to website: https://www.gov.pl/web/protegosafe/jak-to-dziala/

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.

Link to relevant legislation:
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000567/U/D20200567Lj.pdf

Details: The Act of 31 March 2020 on amending certain laws on the health care system related to the prevention, counteraction and combating COVID-19. By virtue of Article 15, a new Article 7e(1) has been introduced in the Act of 2 March 2020 on special solutions related to the prevention, counteraction and combating COVID-19, other infectious diseases and crisis situations caused by them (Journal of Laws, item 374), which concerns the legal obligation to use an application to confirm the execution of the quarantine compliance duty.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks: The DPIA conducted by the Ministry of Digital Affairs contained measures taken to ensure the compliance of the processing with the General Data Protection Regulation and to ensure the data subject's rights. The conducted DPIA did not reveal any risks.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

The installation and use of the ProteGO Safe application takes place on a voluntary basis.
In the application Bluetooth technology is used.
In case of this application, Apple/Google framework is used, based on mixed approach (hybrid/mixed). The developers note that: „This solution is not 100% decentralized, because in order to analyze, among others, the "quality" of contact between devices, the application needs to perform such an operation on a central server (opt-in). This approach is dictated by the need to extend the use of applications to older devices on which such analysis would be difficult or impossible. The mixed approach is currently being discussed in the eHealth network. The European Data Protection Supervisor himself stated explicitly that even in the case of "fully" decentralized solutions, some external server is involved in processing operations. The application tries to process an absolute minimum of data on the server in order to provide greater support for the application by users' devices and to authenticate the transmission of information about contact with

the device of a person suffering from COVID-19. The application server and the registry server for people infected with COVID-19 are independent of each other."

The specifications of the application, in Polish only, is available at: https://github.com/ProteGO-Safe/specs.

The report on ProteGO Safe application security audit of 20 July 2020 is available (in Polish) at: https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport

The application does not require to give any personal data at any stage of use of the application. It does not collect personal data either. All the information processed by the application are processed in a way making the identification of users completely impossible

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

As regards ProteGO Safe application, the Personal Data Protection Office was only indirectly involved - the Ministry of Digital Affairs has consulted the Personal Data Protection Office on the application and its general functions. However, it needs to be noted that, according to the declaration by the Ministry of Digital Affairs, the application was developed among others based on the guidelines of the European Data Protection Board, the European Commission and Toolbox created with the EC eHealth Network which were consulted with UODO.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The Personal Data Protection Office promotes and recommends following the European Data Protection Board's Guidelines regarding contact tracing applications.
Links to relevant information in Polish:
https://uodo.gov.pl/pl/138/1570
https://uodo.gov.pl/pl/138/1495

The Personal Data Protection Office issued a recommendation regarding the general use of applications: https://uodo.gov.pl/en/553/1143

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

As regards the ProteGO Safe application, please see relevant information under points 3.2, 3.3 and 3.6.

According to the information on the government website regarding the ProteGO Safe application (https://www.gov.pl/web/protegosafe/pytania-i-odpowiedzi):

- The use of the application is not connected with the processing of your personal data. The application is neither using nor collecting your personal data.
- The application DOES NOT track a user. No authentication, e.g. giving a telephone number, is required for its activation. The application does not conduct surveillance, does not collect and does not disclose users' data. The information on the encountered devices does not contain any data on their owners, and is anonymous and encoded, and additionally it is stored only on the telephone, for two weeks; then it is erased.
- The application is built according to the principles resulting from the General Data Protection Regulation, including data minimisation, privacy by design, privacy by default, accuracy, integrity and confidentiality.
  The bases are the guidelines of the European Data Protection Board, the European Commission

and Toolbox developed within the European Commission's eHealth network. Special attention is paid to ensuring the highest privacy standards.
- The application was in 100% developed thanks to the coalition of the Polish IT companies working on behalf of government institutions. Google and Apple, as developers of the most popular operational systems, make available only a mechanism allowing for assessment of infection risk. They do not have access to any personal data and are not able to identify users. The application is not linked to any other services (such as iCloud or Google Drive).

The following measures were taken to mitigate the privacy risks in case of the ProteGO Safe application:
- Measures taken to ensure the lawfulness principle
- Measures taken to ensure the purpose limitation principle
- Measures taken to ensure the personal data minimisation principle
- Measures taken to ensure storage limitation principle
- Measures taken to fulfill the information obligations towards the data subject according to the Art. 12, 13 and 14 of the GDPR

According to the Ministry of Digital Affairs the application does not process any personal data.
- Measures taken to implement the right of access by the data subject
- Measures taken to exercise the right to obtain a copy of the personal data undergoing processing
- Measures taken to exercise the right to data portability
- Measures taken to exercise the right to rectification
- Measures taken to exercise the right to erasure of personal data (right to be forgotten)
- Measures taken to exercise the right to restriction of processing
- Measures taken to exercise the right to object to processing of personal data

The second application introduced by the Government is the Home Quarantine ("Kwarantanna domowa") application, which is an obligatory application for persons in quarantine due to a suspected SARS-CoV-2 virus infection that aims to ensure compliance with the quarantine obligation imposed by decisions of the competent authorities. The Act of March 2, 2020 on specific solutions related to the prevention, counteracting and combating of COVID 19, other infectious diseases and crisis situations caused by them (so called "Covid Act") introduced the obligation to install the "Home Quarantine" application which collects i.e. location data. A person in quarantine due to a suspected SARS-CoV-2 virus infection is required to install on his/her mobile device the software provided by the Minister of Digital Affairs to confirm compliance with the quarantine obligation. Information on the application is available on the government website: https://www.gov.pl/web/koronawirus/aplikacje-mobilne According to the information provided by the Ministry of Digital Affairs to the Polish Ombudsman in the letter of 30 November 2020, the Minister of Digital Affairs, as the controller of personal data of the users of the "Home Quarantine" application, when designing the application, made every effort to ensure appropriate technical and organisational measures. In technical terms, data encryption was used, as well as encryption of communication between the application and the environment on which the data are stored. Administrative access to the application is restricted to essential technical staff only, who connect via secure connections from a restricted IP list. The application was also subjected to Privacy by design (Article 25(1) GDPR) and Privacy by default (Article 25(2) GDPR) and DPIA (Article 35 GDPR) procedures, among others, and their results were consulted with the Data Protection Officer of the Ministry of Digital Affairs.

Link to the letter of Ministry of Digital Affairs (in Polish):
https://www.rpo.gov.pl/sites/default/files/Odpowiedz_MC_30.11.2020.pdf

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Ms Teams, Zoom, Google Meet, Librus, ClickMeeting

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Yes.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Account theft, identity theft, lack of appropriate security software, lack of strong passwords

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

Good practices that help keep data secure during online lessons
20 security principles that should be kept in mind by school controllers as well as teachers and students when preparing for online lessons to protect their data

1. Keep your operating systems updated.
2. Regularly update anti-virus, anti-malware and anti-spyware software.
3. Regularly scan workstations with anti-virus, anti-malware and anti-spyware software.
4. Download software only from manufacturers' websites.
5. Do not open attachments sent by email from unknown sources.
6. Do not save passwords in web applications.
7. Do not write down your passwords.
8. Do not use the same passwords in different IT systems.
9. Secure servers or other network resources.
10. Secure wireless networks - Access Point.
11. Adjust the complexity of passwords adequately to the threats.
12. Avoid accessing unknown or contingent websites.
13. Do not log in to IT systems from random places using untrusted devices or public unsecured Wi-Fi networks.
14. Perform regular backups.
15. Use proven software to encrypt emails or storage devices.
16. Encrypt data sent by email.
17. Encrypt hard drives in portable computers.
18. For remote work, use an encrypted VPN connection.
19. When leaving the computer, log out from your device.
20. Do not use random USB storage devices: they may contain malware.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Security of personal data during remote learning – UODO's guide for schools, https://www.uodo.gov.pl/en/553/1118, https://uodo.gov.pl/pl/138/1473

Remote work of teachers and personal data protection - advice for teachers, https://www.uodo.gov.pl/en/553/1137

Protection of personal data when working remotely https://uodo.gov.pl/pl/138/1459

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

The Personal Data Protection Office has issued guides and recommendations (see point 4.6) as well as conducted webinars on safe online lessons – webinars for teachers, e.g. https://uodo.gov.pl/en/553/1137

Québec, Canada - Commission d'accès à l'information du Québec

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Not yet, but it is being planned / considered by the government.

For domestic activities
Not yet, but it is being planned / considered by the government.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

No.

All requirements are issued by the federal government, not by our provincial jurisdiction.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: COVID Alert
Link to website: https://www.quebec.ca/en/health/health-issues/a-z/2019-coronavirus/covid-alert

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:

- Unauthorized access or release of personal information

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Confidentiality and security

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

The authority has provided an opinion to the government and issued recommendation to address privacy risk before the implementation.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

All Federal, Provincial and Territorial Privacy Commissioners from Canada issued a joint statement on may 7, 2020.
https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/

3.9 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.**

NIL.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Do not know.

San Marino - San Marino Data Protection Authority

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: San Marino Digital Covid Certificate
Link to website: https://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17125439.html

1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

For domestic activities
Voluntary.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?

Rating (on a scale of 1 – 5): NIL.

1.5 Please list out the personal data involved in the ‘health passport’ or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: Tables A, B, C, D of the Decree-Law n. 105/2021

For domestic activities
Personal data involved: Tables A, B, C, D of the Decree-Law n. 105/2021

1.6 Is the data collected by the ‘health passport’ or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details: Data will be stored in a Social Security Institute (ISS) server of the Republic of San Marino.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

NIL.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Details: We result that the Congress of State, having heard the opinion of the Executive Committee of ISS and the President of San Marino Innovation, with its resolution, can issue new versions of Tables A, B, C and D and Annex 1 to Law Decree 105/2021 (art. 4 paragraph 6 Law Decree 105/2021)

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

No.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

Bilateral agreements are in place with the EU and other countries with which the Republic of San Marino has diplomatic relations.
The Republic await the approval of the protocol with the EU.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Digital signature according to the standards of the E.U.; data encryption process; the information available in the QRCode is the minimum data for the recognition of the owner of the certificate. The set of minimum data is deprived of the link to the rest of the citizen's personal data.
QRCode Universal allows access with blockchain technology to the portal that still contains the minimum information.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

The Government and other public bodies should consult the San Marino DPA.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No, at the moment.

1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**

Implementation of verification applications according to E.U. standards.
We do not store information.

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements
Testing for COVID-19.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

The risks are the most common but at the same time relevant, namely, wrong processing of the data subjects' information by the controller and the processor.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Audits will be conducted by health or law enforcement personnel only.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

The Government and other public bodies should consult the San Marino DPA.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No; we spread the Compendium of Best Practices in Response to COVID-19 issued by GPA to the Government and other public bodies.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

Audits will be conducted by health or law enforcement personnel only.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

No.

4. Handling of children's or students' data in e-learning technologies

NIL.

Switzerland - Federal Data Protection and Information Commissioner (FDPIC)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: COVID certificate

Main purpose(s):
The COVID certificate is a way of documenting that a person has been vaccinated for COVID-19, have had the disease or have a negative test result.

Description:
The goal of the "COVID certificate" is to facilitate safe travel during the Covid 19 pandemic. The COVID certificate serves as a vaccination, test or recovery certificate. The certificate is interoperable with the EU's and mutually recognized in all EU member states. It is needed for international passenger transport (cross-border air, rail and sea travel).

Link to website:
https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/covid-zertifikat.html#-1821072936

For domestic activities
Name: light certificate

Main purpose(s):
The data-minimised alternative to the COVID-19 certificate was developed at the request of FDPIC, as third parties could use self-developed apps to view health data such as vaccine or date of vaccination when checking COVID-19 certificates. This is prevented with the "light certificate".

Description:
It is in use for domestic events according to the pandemic situation. The "certificate light" is a function in the COVID Certificate app. If the user activates the certificate light, on the basis of the data in your normal COVID certificate a new QR code is created that does not contain health data. The certificate light can only be used in Switzerland. For data protection reasons the certificate light must be activated again after 48 hours. You can deactivate the certificate light any time to return to the normal COVID certificate.

Link to website:

- Federal Office of Public Health:
  - https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/covid-zertifikat.html
  - https://foph-coronavirus.ch/certificate/
- FDPIC's Press Release: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-84262.html

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

Details (if applicable):
The COVID-19 certificate is intended to facilitate the free movement of persons within the EU. However, it is not a requirement for free movement.

For domestic activities
Voluntary.

Details (if applicable):
The Covid certificate can be carried voluntary in the "COVID Certificate" app, PDF or on paper.

The use of the COVID certificate is divided into three zones:

- This certificate is mandatory for:
  - Large events (1,000 persons or more)
  - Clubs, discotheques and dance events
- According to the pandemic situation the certificate can be obliged for:
  - Bars and restaurants
  - Public events with an audience or spectators (up to 1,000 people)
  - Trade and consumer fairs with more than 1,000 visitors
  - Leisure, sport and entertainment establishments such as theatres, cinemas, casinos, swimming pools, etc.
  - Sports and cultural club activities
- The certificate is not foreseen for:
  - Public transport
  - Retail establishments
  - Private events
  - Religious events and political campaign events
  - Personal services such as hairdressing salons, therapeutic and advisory services, etc.
  - Workplaces (including canteens)
  - Training and educational facilities (including canteens)
- https://foph-coronavirus.ch/certificate/where-can-the-covid-certificate-be-used/
- https://www.fedlex.admin.ch/eli/cc/2021/325/de

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 4

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel

Personal data involved:

Besides the person's first and last names, date of birth and a certificate number, the COVID certificate contains details of their COVID-19 vaccination, recovery, or negative PCR or rapid antigen test.

https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/covid-zertifikat.html#-1821072936

Parties having access to the data:

The COVID Certificate Check app is provided to enable the authenticity and validity of COVID certificates to be verified. The data is not stored in a central system. It is only stored on the mobile device and is not transferred in the checking process.

For domestic activities

Personal data involved:

The data-minimized certificate contains only the surname, first name and date of birth of the person concerned, the identification as a data-minimized Swiss Covid 19 certificate as well as the end of the validity.

Parties having access to the data:

Only the user has access, because the data for the "certificate light" is aggregated by the app.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

Details:

- Covid certificate is not stored in any central system. The data is exclusively in possession of the user. In case of loss, the user must request the Covid certificate again from the record office/issuing office (medical person, doctor, etc.) where they were vaccinated or tested.
- During the checking process, the app does not store any data on central systems or in the "COVID Certificate Check" app.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted

The data protection has been taken into account within the general IT Risk Assessement that was conducted by the responsible authority within the process of the development of the application.

Major privacy risks:

Forgery-proof, inalterability, verifiable, no central data storage, internationally compatible, revocability, secure transmission to certificate holders, possibility of ongoing adjustment of validity rules

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

No.

Details: It is not mentioned in the regulation. It is in the competence of the lawmakers respectively of the Federal Office of Public Health. Public security testing is foreseen frequently.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

No.

Details: The certificates are only valid for maximum of 12 months.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

The Confederation operates a system for issuing Covid 19 certificates that is compatible with the "EU Digital Covid Certificate". In the EU, the public key of the Confederation is deposited for verification.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

- **Reduced data set for domestic use (data minimization)**:
  - Checker App: Verify the certificates for authenticity, integrity and validity without transmitting or storing personal data.
- **Transfer of the certificate**:
  - The certificate in paper form can be handed over in person or sent by mail. In the case of transmission by electronic transmission, the issuers must in the case of issuance of Covid 19 certificates ensure that third parties cannot obtain knowledge of the information contained therein.
- There is no obligation for the use of an electronic device. User should have always the opportunity to have the certificate on a paper.
- **Transparency**:
  - The source code and technical specifications of the software are public (open source) without implemented backdoors.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

- Issue statements in connection with the implementation of the certificate in advance
- Monitoring of the implementation of data protection principles
- Participation in the adoption of the legal regulation for the certificate

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes.

Regarding the development of the Covid-19 Certificate the FDPIC issued the following advices:

- Reduced data set for domestic use
- Secure authentication
- Certificate must always be issued in paper form on request
- Definition of minimum standards for data security

No public link available.

1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**

- Minimisation of the collection and retention of personal data
    - *The data-minimized alternative to the Covid 19 certificate was developed at the request of the Federal Data Protection and Information Commissioner (FDPIC)*
    - *FDPIC was successful in being commissioned to develop a second, data-saving QR code for domestic use in addition to the EU-compatible QR code for cross-border traffic. This second code makes it impossible to circumvent data minimisation when reading the certificate. Those who use this second code prevent unauthorised persons from being able to identify the reason why their certificate is shown as valid or invalid by using unauthorised software when reading it. For example, access controllers at a large event do not need to know whether certificate holders are seeking entry as a result of vaccination, convalescence or testing.*
    - *This is prevented by means of the "Certificate Light".*

- Ethical concerns, such as the risk to discrimination and the right to liberty of movement
    - *The FDPIC mentioned repeatedly that the right of movement shouldn't be dependent of showing a Certificate.*
    - *The certificate can be used not only in electronic but also in paper form*

- Use and disclosure limitation, preventing misuse for further incompatible purposes
- Measures to prevent data in the 'health passports' or similar measure(s) from being tampered with
- Adequate safeguards for cross-border data transfers
- Interoperability of the 'health passports' with those in other jurisdictions
- Open Source to avoid backdoors
- Successful IT security test / penetration test

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19
- Others: The persons must record their contact data and complete a form before entry Switzerland by airplane on https://swissplf.admin.ch
  Regulation: https://www.fedlex.admin.ch/eli/cc/2021/380/en#art_1

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Travel companies (Rail, bus, ship or airline operators) are not allowed to retain personal data longer than needed. They shall retain the contact data for 14 days and thereafter destroy the data.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Minimisation principle: There shouldn't be more data retained from the authorities and companies than is needed.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Our focus has been on comments in the legislative process and in the context of consultations during the implementation of legal regulations.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The federal office of Public Health offers a platform "travelcheck" for information purposes:
All travellers must take note of the health-related measures at the Swiss border. The interactive travel check tool on https://travelcheck.admin.ch/home shows what measures apply to the traveller. Thanks to the platform,travellers receive individual information, what their obligations/rights are.

Summary:
If a person has entered a country with a variant of concern in the last 10 days before entering Switzerland, and have the person not been vaccinated or is unable to prove that they have recovered from COVID-19 in the last 6 months, they must go into quarantine after entering Switzerland. After arrival, these people have to go immediately home or to other suitable accommodation (e.g. a hotel or holiday apartment). On the way there, keep a minimum distance of 1.5 metres from other people. The person has to inform the cantonal authority within two days. For 10 days after the arrival in Switzerland, the person must stay in their home or other suitable accommodation according to the document instructions on quarantine. The cantonal authorities are responsible for monitoring the quarantine and can punish by a fine up to CHF 10'000.00. More questions are answered by the link FAQ.

On the Link of the FOPH are more information for entering Switzerland:

- https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-

ausbrueche-epidemien/novel-cov/empfehlungen-fuer-reisende/quarantaene-einreisende.html (English)

Graphic overview about measures:

- https://www.bag.admin.ch/dam/bag/en/dokumente/mt/k-und-i/aktuelle-ausbrueche-pandemien/2019-nCoV/einreise-grafik-massnahmen.pdf.download.pdf/Regeln-Einreise_EN.pdf

To the Ordinance:
Ordinance on Measures to Combat the Coronavirus (COVID-19) in International Passenger Transport

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

NIL.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Proximity-Tracing-App DP-3T
Description:
The app only collects contact events where the user has been in the vicinity of other app users for a short period of time. The contact events are stored decentrally on the user's own mobile phone in the form of a cryptographically generated checksum for 14 days. After 14 days is the data irrevocably deleted. Thus no personal data, locations and information on the device used are exchanged.

The collected data on a user's mobile phone about other users is only stored on the user's mobile phone. It is processed and stored exclusively on the mobile phone. No location data is obtained or processed in any other way. The source code and the technical specifications of all components of the application are public.

If a person tests positive for coronavirus, an authorised agency may with the consent of the infected person request a unique activation code with time-limited validity from the code management system. All the people with whom that person was in contact in previous days – less than 1.5 meters proximity for more than 15 minutes – are alerted via the app to isolate themselves and get tested. The DP-3T system is decentralized.

Link to website: https://foph-coronavirus.ch/swisscovid-app/#function

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.

Link to relevant legislation:
Art. 60 LEp (French)
Ordinance on the Proximity Tracing System for the Sars-CoV-2 coronavirus (English)

Details: The Ordinance regulates the details of the organisation, operation and data processing of the Proximity Tracing System

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
The data protection impact assessment report is on Github (here) public available.

The major risks are: On page 38-42

- Unlawful access of data
- Learning the identity of infected close contacts (identification)
- Users not being notified that they have been exposed
- Users being falsely notified that they have been exposed
- Revealing usage of the Users App and tracking Users's devices
- Backend server can identify infected Users
- Gathering of information about Users through local phone access
- Gathering of significant number of EphIDs through relay attack
- Reuse of the data for new purposes / function creep / mass surveillance
- DP-3T System and technology does not function as anticipated
- Freedom restrictions when not using the User App

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

- Privacy by design/default
- Voluntariness
- Minimisation of data processing and storage
- Data Security
- purpose binding
- Integrity and confidentiality
- Legal Basis

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

FDPIC is the supervisory authority. In this role, it gave feedbacks in the deployment of the application and continues to monitor the tracing app.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

On 21 April 2020, the FDPIC insisted on a legal basis before the introduction of the application.

Update Proximity Tracing App 30.4.2020 (German only)
Update Proximity Tracing App 13.5.2020 (German only)
Update Proximity Tracing App 12.6.2020 (German only)

3.9 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.**

- Minimisation of the collection and retention of personal data: Data is only stored for 14 days and only proceeded on the smartphone. There is anonymized data available for statistics
- A decentralised approach to data storage and processing: Data is not stored on servers.
- Transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy): The code is open source available on github.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Do not know.

In Switzerland, regulation and data protection supervision of the school system is the responsibility of the 23 cantonal authorities (see www.privatim.ch). It is the sovereignty of each canton to determine the technology and teaching materials.

Turkey - Turkish Personal Data Protection Authority (KVKK)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name: Healthpass application
Main purpose(s):
EU published “Digital Green Certificate” application on 17th March 2021 which aims to submit the certificate containing health information in transit among EU Members and makes people exempt from measures such as PCR test and quarantine, provided that they comply with the rules. Health Pass Application is developed for making Digital Green Certificate operational and establishing “Health Passport System” and enabling people to share their personal data with the relevant airlines companies and public authorities.

Description:
It is an application that creates a safe environment with the opportunity to share personal health data such as vaccination, immunity status and test results to be used in Turkey and international travels.

Link to website:
https://healthpass.saglik.gov.tr/ (It is planned that it will be available in application stores in a short time.)

For domestic activities
Name: Life Fits into Home Application
Main purpose(s):
Minimizing the spread of the Pandemics in Turkey, also facilitating and accelerating the adaptation process of Turkish citizens to a controlled social life.

Description:
It is an application developed for the purpose of informing and guiding Turkish citizens about the Covid-19, minimizing the risks related to the Covid-19 and preventing the spread of Covid-19.

Link to website: https://hayatevesigar.saglik.gov.tr/ (The compatible application with mobile devices is available in the Application stores for downloading.)

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Details (if applicable): The Turkish Ministry of Health is in the position of a service provider and no obligation has been imposed by the Ministry. It should be also evaluated within the scope of the targeted countries' conditions by the Health Pass app users.

For domestic activities
Details (if applicable): Obligations are under the jurisdiction of the Ministry of Interior. Life Fits into Home Code Inquiry Service Integration is carried out by the Ministry of Health for performing healthcare services.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): NIL.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: Identity, contact, health, transaction security, visual and audio recording data are processed.

Parties having access to the data: Personal data is not stored in the backend in any way and is not shared with third parties.

For domestic activities
Personal data involved: Identity, contact, location, health and occupational data are processed.

Parties having access to the data: Based on the legal reason mentioned in the third paragraph of Article 6 of the Personal Data Protection Law (No.6698), "*Personal data, except for data concerning health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws. Personal data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by the persons subject to secrecy obligation or competent public institutions and organizations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing*." the personal data is shared with the authorized institutions and organizations in order to protect public health and prevent the spread of the Covid-19.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

No, decentralised storage on users' devices is adopted.

Details: Within the scope of Life Fits into Home Application, personal data is encrypted with a one-way encryption algorithm and stored in the central database in order to protect public health and prevent the spread of the Covid-19.

No personal data is stored in the central database within the scope of the Health Pass Application.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Major privacy risks:

Health Pass Application:
In the every phases of Health Pass Application, relevant works have been performed in accordance with the general principles in the Article 4 of Personal Data Protection Law and technical and organisational measures in the Article 12 of the Law have been taken.

No personal data is stored in the database.

Life Fits into Home Application:
In the every phases of Application, relevant works have been performed in accordance with the general principles in the Article 4 of Personal Data Protection Law and technical and organisational measures in the Article 12 of the Law have been taken. Since it is hard to ensure privacy in the scenario of capturing Turkish Republic Citizenship Number which is constant, "Life Fits Into Home Code" system which provides personal, unique and user-managed code has been formed for the preclusion of risks. Personal data which has been stored in the data banks are kept encrypted through one-way encrypting algorithm.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

Yes.

Details: Both applications are regularly maintained and improved.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

Yes.

Details: Personal data processing activities within the scope of Life Fits into Home Application has been planned to be limited with the duration of the Covid-19 Pandemics.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

There is no cross border transfer within the Health Pass and Life Fits into Home applications.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

The following principles that shall be in accordance with the processing of personal data pursuant to Article 4 of the Personal Data Protection Law are applied:

- Lawfulness and fairness.
- Being accurate and kept up to date where necessary.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

Views have been exchanged with the relevant stakeholder.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NIL.

1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**

- Transparency requirements are met in the development and use of applications. Informing note and privacy policy have been created and made available to users.
- Applications are designed to minimize the collection and storage of personal data.
- In the Applications, measures have been taken to ensure that personal data is processed limited to the purposes of processing.
- Technical and organizational measures specified in the Law are taken (e.g., personal data used in Life Fits into Home Application are processed using one-way encryption algorithms. Personal data is not stored in a central database of the Health Pass Application).
- Necessary measures are taken to prevent unauthorized (external) access to personal data processed within the both applications.
- There is no cross border transfer within the Health Pass and Life Fits into Home applications.
- In the development and operation processes of the applications, the Information Security Policies of Ministry of Health (indicated in the "Information Security Policy Instruction of the Ministry of Health" and "Information Security Policy Guidelines of the Ministry of Health") are implemented. (For example, secure software development principles have been applied during the software development process. Applications have been subjected to vulnerability scanning and penetration tests to be safe against all kinds of external attacks. Required log records are stored for the application security.)

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Testing for COVID-19
- Others:
  For entering Turkey, filling Entry Form and being tested for COVID-19 are mandatory but if there is certification of vaccination or a document that shows the person who is incoming traveller or returning national had COVID-19 before, COVID-19 test is not applied. Conditions for entering countries and mandatory quarantine can change according to regulations between countries. (It should be taken into consideration that the requirements specified above are current measures and they may be changed.)

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

NIL.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

The following principles that shall be in accordance with the processing of personal data pursuant to the general principles in the Article 4 of the Personal Data Protection Law are applied:

- Lawfulness and fairness.
- Being accurate and kept up to date where necessary.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

NIL.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NIL.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

In the every phases of Health Pass Application, relevant works have been performed in accordance with the general principles in the Article 4 of Personal Data Protection Law and technical and organisational measures in the Article 12 of the Law have been taken.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?

- Bluetooth technology
- GPS location tracking

What best describes the approach used to build the contact tracing app?

Centralised approach.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Life Fits Into Home Application
Description:
It is an application that is developed for the purpose of informing and guiding the citizens on Coronavirus (COVID-19), minimizing the risks regarding the communicable disease and preventing its spread.
Link to website:
https://hayatevesigar.saglik.gov.tr/ (The compatible application with mobile devices is available in the Application stores for downloading.)

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Major privacy risks:
In the every phases of Application, relevant works have been performed in accordance with the general principles in the Article 4 of Personal Data Protection Law and technical and organisational measures in the Article 12 of the Law have been taken. Since it is hard to ensure privacy in the scenario of capturing Turkish Republic Citizenship Number which is constant, "Life Fits Into Home Code" system which provides personal, unique and user-managed code has been formed for the preclusion of risks. Personal data which has been stored in the data banks are kept encrypted through one-way encrypting algorithm.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

The following principles that shall be in accordance with the processing of personal data pursuant to the general principles in the Article 4 of the Personal Data Protection Law are applied:

- Lawfulness and fairness.
- Being accurate and kept up to date where necessary.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Views have been exchanged with the relevant stakeholder.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

NIL.

3.9 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.**

In the every phases of Application, relevant works have been performed in accordance with the general principles in the Article 4 of Personal Data Protection Law and technical and organisational measures in the Article 12 of the Law have been taken.

In consideration with the best practices in the Annex; conducting of data protection/privacy impact assessment and other risk assessment prior to rolling out the contact tracing app, and regular audit and reassessment, minimisation of the collection and retention of personal data, prohibiting against misuse of personal data for incompatible purposes, data security measures, transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy), processing personal data limited with the efficacy and effectiveness of the contact tracing app (e.g. retention of contact tracing data limited with risk period and termination after this period ends).

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

Education Informatics Network (EBA), Zoom.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

NIL.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

It is seen that, in distance learning platforms, personal data such as names and surnames of the students as well as some special categories of data that can be evaluated within the scope of biometric data such as voice and image, are processed.

Furthermore, it is observed that much software that is used for distance learning provides services through cloud service providers and the data centers of such software are mostly located abroad.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

The following principles that shall be in accordance with the processing of personal data pursuant to the general principles in the Article 4 of the Personal Data Protection Law are applied:

- Lawfulness and fairness.
- Being accurate and kept up to date where necessary.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes. Link is provided below:
https://www.kvkk.gov.tr/Icerik/6725/Public-Announcement-on-Distance-Learning-Platforms

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

NIL.

United Kingdom - Information Commissioner's Office (ICO)

1. 'Health passports'

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Yes.

For domestic activities
Yes.

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel
Name:

- England:NHS COVID Pass
- Wales: Vaccination certificate request to local health board
- Scotland: Vaccine certificate request from NHS inform website
- Northern Ireland: No current measure, paper based format being worked on

Main purpose(s): To show coronavirus vaccination details or test results
Description: Digital version using NHS app or website, paper version (vaccination status only)
Link to website: NHS COVID Pass for events and travel - NHS (www.nhs.uk)
Get a record of your coronavirus (COVID-19) vaccination status | The coronavirus (COVID-19) vaccine (nhsinform.scot)

For domestic activities
Name: NHS COVID Pass
Main purpose(s): Currently used for events where COVID Pass is being trialled
Description: Digital version using NHS app or website, paper version (vaccination status only)
Link to website: NHS COVID Pass for events and travel - NHS (www.nhs.uk)

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

For domestic activities
Voluntary.

Details (if applicable):
It is (at the time of writing) voluntary to use the COVID pass for large event trials, however, attendees must be able to demonstrate they have had a recent negative test outside of that system should they choose not to use it.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5): 4

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

For cross-border/boundary travel
Personal data involved: NHS number, name and COVID-19 vaccination history
Parties having access to the data: Accessed only via the NHS service

For domestic activities
Personal data involved: NHS number, name and COVID-19 vaccination and test result history
Parties having access to the data: Accessed only via the NHS service

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.

Yes, centralised storage is adopted.

Details: The NHS in England hold a central COVID-19 vaccination database. Test results are also held in a national database. Data is pulled from these stores.

1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks: Feedback provided on DPIA submitted for the trial events. Retention period was unclear, anonymisation of data was not assured, lack of clarity around lawful basis, specifically relying on consent. Lack of clarity re controller and processors.

1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.

No.

1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.

No.

Details: Policy in this area is yet to be determined by the UK government.

1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?

None at present. No interoperability across the UK nations either.

1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

Necessity, proportionality, scope creep, data minimisation and retention.

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

Regular contact with NHSX and government departments. Reviewed DPIA and privacy notices and provided feedback.

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Expectations document published 'COVID-status certification: data protection expectations'. This sets out the ICO's expectations on how organisations may develop certification schemes in line with the principles of data protection by design and default.
covid-status-certification-dp-expectations.pdf (ico.org.uk)

1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**

Lawful and fair – use is not mandatory to avoid discrimination
Clear purpose – to avoid scope creep, at present use of for international travel and entry to trial events only
Obtain minimum amount of personal data necessary and store for minimum amount of time

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

Yes.

Relevant requirements

- Mandatory quarantine
- Testing for COVID-19
- Others:
  Before entry into the UK, you need to complete a passenger locator form 48 hours prior to arrival. What you then need to do depends on where you have been to or passed through in the 10 days before you arrive. A traffic light system has been or introduced where countries/territories are classified as red, amber or green. The system applies to England with Scotland, Wales and Northern Ireland able to make their own rules. However, the rules adopted are broadly the same. If you have been to or passed through a country on the green list you must take a COVID-19 test on or before day 2. If on the amber list you must quarantine in the place you are staying and take 2 COVID-19 tests. If on the red list you must quarantine in a hotel for 10 days and take 2 COVID-19 tests. You cannot currently enter the UK if you have been in or through a country on the red list unless you are British, Irish or have the right to live in the UK. There are exemptions from some or all of the COVID-19 travel and entry requirements because of your job.

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

Risk of intrusive surveillance to ensure compliance with quarantine measures.

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

Necessity, proportionality, scope creep, data minimisation and retention.

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

Meetings with the Home Office, Department of Transport. Reviewed and provided feedback on the Covid-19 Charter. This provides information on consumer rights, responsibilities and reasonable expectations for international travel while Coronavirus restrictions remain in place.

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

No.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

NIL.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?
Bluetooth technology.

What best describes the approach used to build the contact tracing app?
Exposure Notification API built by Google and Apple.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name:
- England: NHS Test and Trace
- Scotland: Test and Protect
- Wales: Test, Trace, Protect
- Northern Ireland: Contact tracing service

Link to website:
NHS Test and Trace (phe.gov.uk)
Test and Protect | NHS inform
Test, trace, protect: coronavirus - Public Health Wales (nhs.wales)
Contact tracing | HSC Public Health Agency (hscni.net)

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

Yes, new legislation was introduced.

Link to relevant legislation:
The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020 (legislation.gov.uk)

Details: Hospitality venues required by law to collect contact details of customers and visitors.

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

Major privacy risks:
R009 – Malicious access to backend data base through cyberattack
R014 – Inability to exercise data subject rights
R016 – Unauthorised disclosure of health status to others
R017 – Disclosure (identification) of app users through linking app data to information held in the outside world.
(All medium/amber risks which were reduced further through controls)
The NHS COVID-19 app (Late April 2021 release) (publishing.service.gov.uk)

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

Be transparent about purpose, design choices and the benefits. Collect minimum amount of personal data necessary, protect users and give them control, keep data for minimum amount of time and where appropriate ensure user has control over this. Securely process the data, ensure user can opt in or out without any negative consequences. Strengthen privacy and don't weaken it.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Conversations with NHSX regarding app and associated activities in the planning stages. Issuing timely guidance and advice as below.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Yes, expectations document, blog and formal opinion published
COVID-19 Contact tracing data protection expectations on app development (ico.org.uk)
Blog: Data protection considerations and the NHS COVID-19 app | ICO
Apple and Google joint initiative on COVID-19 contact tracing technology (ico.org.uk)

3.9 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.**

All data collected must comply with UK GDPR and will not be kept for longer than necessary. Data collection should be as straightforward as possible for organisations. Contact details will only be shared with NHS Test and Trace if it is requested.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, significant or moderate increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

We did receive some enquiries during the pandemic about e-learning technologies, such as the use of cameras/keystroke software to monitor cheating in online mock exams/assessments. However the most popular e-learning technology we noticed emerging through the COVID-19 pandemic was the use of online platforms such as Microsoft Teams to manage and deliver lessons as well as managing homework assignments and other related tasks.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

Under the UK GDPR, DPIA's are a legal requirement for any processing that is likely to result in a high risk, for example the processing of special category data on a large scale. Therefore for some e-learning technologies, a DPIA will need to completed beforehand.

Even if it is not required under the legislation, we would usually still advise that one is completed due to the benefits they bring in assessing compliance and risk and demonstrating accountability.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

- Overly intrusive
- Inadvertent disclosure of personal data/special category data
- Risk of children not understanding what default privacy settings are on the sites and devices they're using.
- Potential security issues

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

The standout ones would probably be fair, lawful & transparent, security and accountability. However all would be applicable and key to consider.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

The ICO has published its Age Appropriate Design Code. Whilst this is not specifically about e-learning technologies, it is about protecting Children and their data within a digital world, it will still have relevant points to consider when considering the adoption of e-learning technologies.

The code sets out 15 standards of age appropriate design, reflecting a risk-based approach. The focus is on providing default settings which ensures that children have the best possible access to online services whilst minimising data collection and use, by default.

4.7 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.**

NIL.

Victoria, Australia - Office of the Victorian Information Commissioner (OVIC)

1. ‘Health passports’

1.1 Does your jurisdiction have a ‘health passport’ or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel
Not yet, but it is being planned / considered by the government.

For domestic activities
No.

1.2 Please provide the name of the ‘health passport’ or similar measure(s), its main purposes and a brief description of how it works (if applicable).

Not applicable.

1.3 Is the use of the ‘health passport’ or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel
Voluntary.

Details (if applicable):
As OVIC understands, work toward an Australian heath passport is in very early stages. At this stage, any Australian health passport will only be relevant for Australians leaving the country.

For domestic activities
Voluntary.

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public’s acceptance of the idea of ‘health passport’ in your jurisdiction?

Rating (on a scale of 1 – 5): OVIC not able to comment at this stage.

1.5 Please list out the personal data involved in the ‘health passport’ or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.

As OVIC understands, the personal data involved in the health passport specifically pertains to COVID-19 vaccine status only.

1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.
OVIC understands that data collected and shared as part of the health passport will only be shared between relevant Australian government agencies.
1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?
OVIC understands that a privacy impact assessment has not been conducted on the health passport from an international perspective (that is, health passports for Australians leaving the country).
1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
No. Details: Given the early stages of the work to develop health passports, not yet.
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
No.
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
At this stage, OVIC is not best placed to comment.
1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?
As OVIC does not regulate health information, nor information sharing within and between federal government agencies, OVIC is not best placed to comment.
1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?
Consultative – OVIC has previously attended discussions with relevant federal government agencies regarding the development of health passports.
1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
Not applicable.
1.14 **What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.**
NIL as of current – OVIC participating in ongoing consultations with relevant federal government agencies.

2. Health monitoring of incoming travellers and returning nationals

As the Health Complaints Commissioner regulates health information in Victoria, OVIC is not best placed to respond to this section.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

Yes.

3.2 Please select the relevant characteristics of the digital contact tracing app:

Use of contact tracing check-in services to locations with a Service Victoria QR code, via the Service Victoria app.

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name: Service Victoria app
Description: Service Victoria is a Victorian government agency that offers access to Victorian government services online.
Link to website: https://service.vic.gov.au/.

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

No legislative change.

Details:
OVIC is not best placed to speak to the legislative authority for Victoria's contact tracing efforts. However, OVIC understands that the Chief Health Officer in Victoria had existing powers under the *Public Health and Wellbeing Act 2008* to facilitate contract-tracing.

Service Victoria's privacy policy notes that the Service Victoria app "provides a digital means for employers/businesses to comply with their obligations under the Workplace Directions of the Chief Health Officer issued under the *Public Health and Wellbeing Act 2008*".

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

Yes, DPIA has been conducted.

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

The Information Privacy Principles under the *Privacy and Data Protection Act 2014*, where applicable.

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

Consultative and regulatory. OVIC attended meetings of a Steering Committee, established by the lead state government agency in Victoria.

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

Not applicable – the Federal Privacy Commission, the Office of the Australian Information Commissioner, is working to publish guidelines on nationally consistent approaches to collecting personal information for contact-tracing: https://www.oaic.gov.au/engage-with-us/consultations/requirements-to-collect-personal-information-for-contact-tracing-purposes/draft-guidelines-requirements-to-collect-personal-information-for-contact-tracing-purposes/.

3.9 **What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.**

Purpose limitation
OVIC has previously noted, while providing evidence to the Legislative Council Legal and Social Issues Committee's Inquiry into the Victorian Government's COVID–19 contact tracing system and testing regime, that it is positive that the information collected for contract tracing purposes under relevant legislation in Victoria can only be used for the purposes of contact tracing.

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

Yes, moderate increase.

4.2 What are the popular e-learning technologies used in your jurisdiction?

OVIC is not best placed to respond. The Department of Education and Training (DET) in Victoria has guidance about online learning tools used in Victoria.

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?

When consulted, OVIC would recommend the completion of privacy impact assessment before implementing any e-learning tool in Victorian schools (or for an existing privacy impact assessment to be revisited, to account for any new uses of personal information that the e-learning tool may result in.

4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?

Some of the privacy risks associated with e-learning tools identified by OVIC include:

- overcollection of personal information via the use of videocall functionalities; and
- unauthorised transborder dataflows or secondary uses of personal information if data is stored in cloud services.

4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?

The Information Privacy Principles under the *Privacy and Data Protection Act 2014*, where applicable.

4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

While not specific to e-learning tools, OVIC issued guidance in 2020 on Collaboration tools and privacy, for the Victorian public sector.

4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.

The DET is best placed to respond. OVIC's regulatory oversight extends to public (government) schools in Victoria.

Annex A: Questionnaire of the Survey on Experience and Best Practices in Response to COVID-19

COVID-19 Working Group

SURVEY ON EXPERIENCE AND BEST PRACTICES IN RESPONSE TO COVID-19

Background

At the 42nd Global Privacy Assembly (GPA) Close Session held in October 2020, the COVID-19 Taskforce (i.e. the predecessor of the COVID-19 Working Group) presented the 'Compendium of Best Practices in Response to COVID-19', which contained relevant experience and good practice contributed by 32 GPA members and observers in relation to several privacy issues arising from the COVID-19 pandemic.

The 42nd GPA Closed Session also adopted the 'Resolution on the Privacy and Data Protection Challenges Arising in the Context of the COVID-19 Pandemic', which, among others, resolved to officially establish the COVID-19 Working Group. One of the COVID-19 Working Group's tasks is to consider, make recommendations for and coordinate the GPA's responses on privacy and data protection issues arising from the COVID-19 pandemic and the road to recovery.

The purpose of this survey is to facilitate the compilation of the second edition Compendium of Best Practices in Response to COVID-19, by collecting from GPA members and observers the key data protection principles, guidance and recommended best practices regarding various emerging privacy issues arising at this stage of the COVID-19 pandemic. The topics covered in this survey are based on the results of the previous *GPA COVID-19 Working Group Survey on Emerging Privacy Issues*, conducted in March 2021 among GPA members and observers.

It is not mandatory to answer all the questions below. If your authority does not have relevant experience or considers it inappropriate to share your experience or views, please state the fact and skip the question(s). Please answer the questions to the best of your knowledge and provide links and references where you consider helpful.

If possible, **please keep your answers concise and in full sentences** to aid the compilation of the Compendium of Best Practices in Response to COVID-19. For some of the questions, you may refer to certain sections of the Annex to guide your response.

We invite you to complete the survey on or before **12 July 2021 (Monday)** and send your return to [redacted].

Basic Information	
Name of your authority:	
Emblem of your authority:	
Your jurisdiction:	

1. 'Health passports'[12]

1.1 Does your jurisdiction have a 'health passport' or similar measure(s) which processes and shares personal data to facilitate cross-border/boundary travel and/or domestic activities?

For cross-border/boundary travel

☐ Yes ☐ No ☐ Not yet, but it is being planned / considered by the government

For domestic activities

☐ Yes ☐ No ☐ Not yet, but it is being planned / considered by the government

1.2 Please provide the name of the 'health passport' or similar measure(s), its main purposes and a brief description of how it works (if applicable).

For cross-border/boundary travel

Name:
Main purpose(s):
Description:
Link to website:

For domestic activities

Name:
Main purpose(s):
Description:
Link to website:

1.3 Is the use of the 'health passport' or similar measure(s) mandatory or voluntary? Please briefly introduce the relevant legal requirements, if applicable.

For cross-border/boundary travel

☐ Mandatory ☐ Voluntary

Details (if applicable):

For domestic activities

☐ Mandatory ☐ Voluntary

Details (if applicable):

1.4 From the perspective of personal data privacy, on a scale of 1 (least receptive) to 5 (most receptive), how do you rate the public's acceptance of the idea of 'health passport' in your jurisdiction?

Rating (on a scale of 1 – 5):

[12] 'Health passports' or 'health codes' generally refer to digital solutions developed to evaluate individuals' COVID-19 infection risks by recording whether they have been vaccinated against COVID-19, received a negative test result or recovered from COVID-19, etc., often in order to facilitate cross-border/boundary travel or domestic activities. For the purpose of this survey, the use of other certificates in paper or digital form to similar effect will also be covered.

1.5 Please list out the personal data involved in the 'health passport' or similar measure(s) (e.g. personal data collected in vaccination programmes such as vaccination status, COVID-19 test results, travel history and contact history, telephone numbers, residential addresses, etc.), and the parties who may have access to the data.
For cross-border/boundary travel Personal data involved: Parties having access to the data: *For domestic activities* Personal data involved: Parties having access to the data:
1.6 Is the data collected by the 'health passport' or similar measure(s) stored or processed in any central databases? Please elaborate.
☐ Yes, centralised storage is adopted ☐ No, decentralised storage on users' devices is adopted Details:
1.7 Has a data protection impact assessment (DPIA) been conducted prior to the setting up of the 'health passport' or similar measure(s)? What are the major privacy risks identified in the DPIA?
☐ Yes, DPIA has been conducted ☐ No, DPIA has not been conducted Major privacy risks:
1.8 Are there any plans to review and evaluate regularly the 'health passport' and similar measure(s) for its efficacy and effectiveness? Please elaborate.
☐ Yes ☐ No Details:
1.9 Are there any policies in place to terminate the 'health passport' or similar measure(s) after the COVID-19 pandemic is over? Please elaborate.
☐ Yes ☐ No Details:
1.10 What are the mechanisms in place to facilitate cross-border transfer of data in the 'health passport' and/or its interoperability with similar measures in other jurisdictions?
1.11 What are the key data protection principles regarding the development and use of the 'health passport' or similar measure(s)?

1.12 What is the role of your authority in the planning for and implementation of the 'health passport' or similar measure(s) (e.g. providing advice during consultation)?

1.13 Has your authority issued any guidance or advice regarding the development and use of 'health passport' or similar measure(s)? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

1.14 What are the measures adopted in your jurisdiction to address or mitigate the privacy risks associated with the development or use of 'health passport' or similar measure(s)? Please provide real examples if possible.

Note: In your response to Q.1.14, you may consider including best practices which may address the following concerns, if applicable:

- Transparency requirements in the development and use of health passports or similar measure(s)
- Minimisation of the collection and retention of personal data
- Use and disclosure limitation, preventing misuse for further incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Measures to prevent data in the 'health passports' or similar measure(s) from being tampered with
- Adequate safeguards for cross-border data transfers
- Ethical concerns, such as the risk to discrimination and the right to liberty of movement
- Efficacy and effectiveness of the 'health passports' or similar measure(s)
- Interoperability of the 'health passports' with those in other jurisdictions

2. Health monitoring of incoming travellers and returning nationals

2.1 Does your jurisdiction have requirements and/or measures to monitor the health of incoming travellers and returning nationals? If yes, please select the applicable requirements.

☐ Yes ☐ No ☐ Not yet, but it is being planned / considered by the government

Relevant requirements

☐ Mandatory quarantine ☐ Reporting body temperature to health authorities

☐ Testing for COVID-19 ☐ Reporting other COVID-19 symptoms to health authorities

☐ Others, please provide a brief description:

2.2 What are the major privacy risks identified by your authority in relation to the health monitoring of incoming travellers and returning nationals?

2.3 What are the key data protection principles regarding health monitoring of incoming travellers and returning nationals?

2.4 What is the role of your authority in the planning for and implementation of measures monitoring the health of incoming travellers and returning nationals?

2.5 Has your authority issued any guidance or advice regarding the health monitoring of incoming travellers and returning nationals? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

2.6 What are the measures adopted in your jurisdictions to address or mitigate the privacy issues associated with health monitoring of incoming travellers and returning nationals? Please provide real examples if possible.

3. Contact tracing measures

3.1 Does your jurisdiction have a digital contact tracing app that tracks or traces close contacts of COVID-19 infected persons?

☐ Yes ☐ No ☐ Not yet, but it is being planned / considered by the government

3.2 Please select the relevant characteristics of the digital contact tracing app:

What are the underlying technologies used in the contact tracing app?

☐ Bluetooth technology ☐ GPS location tracking ☐ Using data from mobile operators

☐ Others, please specify:

What best describes the approach used to build the contact tracing app?

☐ Centralised approach ☐ Exposure Notification API built by Google and Apple

☐ Other decentralised approach ☐ Others, please specify:

3.3 Please provide the name and a brief description of the digital contact tracing app (if applicable).

Name:
Description:
Link to website:

3.4 Has your jurisdiction introduced or amended any legislation to facilitate contact tracing? Please provide details of the relevant law(s) and the main purpose of such legislative action(s).

☐ Yes, new legislation was introduced ☐ Yes, existing legislation was amended

☐ No legislative change

Link to relevant legislation (if applicable):

Details:

3.5 Has a DPIA been conducted prior to the implementation of the contact tracing app? What are the major privacy risks identified in the DPIA?

☐ Yes, DPIA has been conducted ☐ No, DPIA has not been conducted

Major privacy risks:

3.6 What are the key data protection principles regarding the development and use of the contact tracing app?

3.7 What has been the role of your authority in the planning for and implementation of contact tracing app?

3.8 Has your authority issued any guidance or advice regarding the development and use of the contact tracing app? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.

3.9 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the development and use of the contact tracing app? Please provide real examples if possible.

Note: In your response to Q.3.9, you may consider including best practices which may address the following concerns, if applicable:

- Conducting of data protection / privacy impact assessment and other risk assessment prior to rolling out the contact tracing app, and regular audit and reassessment thereafter
- Minimisation of the collection and retention of personal data
- A centralised or decentralised approach to data storage and processing
- Prohibiting against misuse of personal data for incompatible purposes
- Data security measures (e.g. encryption, decentralised data processing, etc.)
- Transparency of the contact tracing app (e.g. publishing information on the contact tracing app and its privacy policy)
- Efficacy and effectiveness of the contact tracing app
- Termination of the contact tracing app and erasure of data collected by the app
- Interoperability of the contact tracing app with similar apps in other jurisdictions

4. Handling of children's or students' data in e-learning technologies

4.1 Did your authority observe an increase in the use of e-learning technologies in your jurisdiction during the COVID-19 pandemic?

☐ Yes, significant increase ☐ Yes, moderate increase
☐ No increase ☐ Do not know

4.2 What are the popular e-learning technologies used in your jurisdiction?

4.3 Does your authority recommend or require DPIA be conducted prior to the adoption of e-learning technologies by education institutions in your jurisdiction?
4.4 What are the major privacy risks identified by your authority in relation to the handling of children's and students' data in the use of e-learning technologies?
4.5 What are the key data protection principles regarding the handling of children's or students' data in the use of e-learning technologies?
4.6 Has your authority issued any guidance or advice regarding the handling of children's or students' data in the use of e-learning technologies? If yes, please summarise briefly the key points and provide the link to the guidance or advice, if available.
4.7 What are the measures adopted in your jurisdictions to address or mitigate the privacy risks associated with the handling of children's or students' data in the use of e-learning technologies? Please provide real examples if possible.
Note: In your response to Q.4.7, you may consider including best practices which may address the following concerns, if applicable: • Assessment of privacy impact or risk assessment by schools • Assessment of the necessity, effectiveness and proportionality of exam monitoring measures and tools • Implementation of the appropriate data security measures in the e-learning tools • Implementation of the adequate safeguards for cross-border transfer of personal data collected by e-learning tools • Policies regarding the recording of audio and video of lessons • Provision of guidance to parents

Annex B: Work of the Sub-group on Regulatory Capacity Building

COVID-19 Protocols Lessons Learned Survey Results Report

Executive Summary of Survey

As part of the response to COVID-19 protocols implementation, a significant amount of personal data and special category data, namely personal health information, has been collected and shared by our employers, businesses, schools, insurance companies, healthcare providers and government agencies. In order to properly understand how well-equipped these organizations were for handling personal data in volumes and ways they have not experienced before, the GPA COVID-19 Working Group surveyed non-privacy regulators, individuals and organizations about the information they provided along with the COVID-19 data collection protocols regarding how to collect it, process it, store it, and share it. The survey set about understanding what data protection authorities or similar regulators could have done better and what they did right. These lessons learned will then be reflected potentially in COVID-19 Working Group guidance, the 2nd edition of the Compendium on Best Practices that Sub-group 1 on Emerging Issues has compiled, and as best practices and suggestions for GPA Members and Observers to issue via their own supervision, guidance and outreach methods.

The resulting lessons learned, set out below the detailed analysis of each thematic area, capture options for regulatory capacity building within the specific context emergency regulatory response, COVID-19 or otherwise. As this is the first major, global emergency scenario in the era of data protection and digital footprint of individuals and governments, it has shown a light on the need to develop an "Incident Response" toolkit for regulators, as well as other ways privacy regulators in particular may take a leading role in such response, given the criticality of the data collected and associated risks.

Main Thematic Areas Reviewed in the Survey

1. Communications and guidance (Q 1 to 5)
2. Organizational/operational impact of COVID-19 restrictions on data subjects' rights (Q6 and 7, 16 to 20)
3. Sharing, Security and breach reporting (Q10 to 14, Q26 to 30)
4. Privacy Tech/IT Development, framework and design (Q20 to 24)
5. Supervision and Enforcement (Q8, 9, 15 and 25)

Survey link: https://survey.alchemer.com/s3/6191656/Global-Privacy-Assembly

Responses and Analysis

1. Communications and Guidance

Overall, regardless of the existence of data protection and privacy laws in the jurisdiction, respondents indicated that additional guidance and clear, consistent implementation measures across all regulators, privacy and non-privacy, would be useful to them. Some suggestions included:

a. providing a holistic document to guide all aspects of not only data protection, security, retention and sharing during in an emergency such as the COVID-19 pandemic, but the larger impact on business / business impact of data breaches;
b. better use of social media to share messaging;
c. checklists with clear instructions for all entities that had to implement new / update old measures; and
d. earlier, more targeted responses

Respondents suggested that the privacy regulators should have more decision-making authority and involvement in the pandemic response protocols. Also, small and medium enterprises with already limited resources, that were then negatively impacted by lock down and the resulting economic downturn, requested additional resources to help decision making. A very clear concern was echoed throughout, regarding online fraud and phishing attacks. One responded stated, "Intensify the fight against the growing number of online fraudsters… exploiting the public fear surrounding the COVID-19, using the pandemic to lure people into clicking phishing emails and installing malware capable of stealing personal data and money."

Lessons Learned:

A coordinated, cross-disciplinary guidance document showing the links between specific regulatory objectives and the underlying privacy and security concerns is needed. Health, education, economic and social objectives in preventing the spread of COVID-19 all have privacy and security issues attached to them, presenting issues that were probably already existing but now have come to light. There is an opportunity to re-visit and improve the way data is managed. Regulatory capacity across all relevant regulators in pandemic / emergency response should be built. When the situation returns to a bit more normal, this collaboration should continue, to build guidance and an emergency incident response plan comprising all facets of regulatory impact: privacy, yes, but also health care, economic / financial, education and other relevant stakeholders.

2. Organizational / operational impact of COVID-19 restrictions on data subjects' rights

While data collection and processing changed in that certain types of sensitive personal data were being collected on a much larger scale, generally it appears that little else changed in that regard. The main change in data collection by organizations at the request of health regulator response requirements was around an increase in health data collection (temperature taking, COVID-19 test results, vaccination records, etc), which should come as no surprise. Respondents clearly indicated by an overwhelming majority response that data subjects' rights

have always and continue to be very important to them within their organizations. A small number of respondents developed new policies and procedures, presumably where none existed before, as a result of COVID-19 response requirements. Some changes were made, but in large part privacy and security policies and procedures remained unchanged. The primary types of safeguards and controls that most respondents supported were based on developing relevant contractual clauses or data processing agreement in order to manage privacy and security requirements.

Lessons Learned:

Regulators should push entities to prioritize policy and procedural reviews due to the increase in a specific type of data collection, i.e., health data. Entities that never collected such data before must have a clear directive about how to collect it and what to do with it once they have it, from sharing to storing to deleting (if ever). Additional types of safeguards may need to be developed as well for processing, as contractual clauses, DPAs and even consent may not be enough to ensure it is managed properly. Work with each other and with other regulators to brainstorm what other safeguards may work to protect such data. Perhaps for example regular technical reviews and audits should be documented on at least an annual basis and spot checked by each regulator on an appropriate scale.

3. Sharing, Security and Breach Reporting

Understandably, government data sharing requests increased quite a bit during 2020, as health and education regulators and facilities sought to learn about who, where and why people were getting infected with COVID-19. Where data sharing requests were made, the purpose and scope of the requests were clear and specific, and the requesting authority, where applicable, was happy to apply appropriate safeguards and controls to the transfers. Most data sharing requests were from either the local health or public safety regulators. Note well, in any case, that over 60% of respondents did not attempt to suggest to the government requesting authority that any controls be applied to the data sharing.

Interestingly, while a small majority of respondents were concerned about enforcement action as a result of privacy issues around COVID-19 response data collection and processing, a large majority thought that nothing should change in terms of privacy and security enforcement action, which, as suggested in the survey, is a key learning tool.

Lessons Learned:

Even before COVID-19, data sharing requests from government agencies posed privacy and security concerns. The pandemic highlighted, however, the need for guidance or perhaps incorporating into legislation the requirement to insist on controls and safeguards specifically where government data sharing requests are made, including contractual clauses accounting for the innate conflict that often exists between public safety and national security objectives and protecting personal data. Very often contractual clauses meet tick box requirements and are much too general to adequately address this conflict. Compliance with laws clauses, as well as "public interest" legislative requirements, potentially weaken the ability to sufficiently

protect personal data. A set of government data sharing policies, procedures and contractual clauses, both general and COVID-19 specific, could be developed to address such concerns.

4. Privacy Tech / IT Development, framework and design

Perhaps unsurprisingly, most respondents said that they are using privacy enhancing technology (PET) such as encryption and two factor authentication in their IT infrastructure. A small percentage are using anonymization/pseudonymization tools or digital signatures. Nearly all respondent jurisdictions have contact tracing apps that are not mandatory to download or use but are user friendly.

Lessons Learned:

Informational fact sheets and other clear, understandable templates and tools may be developed about incorporating PET, privacy engineering and innovative ways to better protect specific data types, such as data collected in response to or as a result of emergency conditions. A playbook for pandemics / emergencies would be useful as well, as part of national planning for emergency response and / or business continuity with respect to IT, security and data protection business critical risks, especially where they all cross over with each other. Keeping a risk register updated with data protection related risks is underrated and underdeveloped in certain regions, as this area of IT compliance and governance still develops. Targeted, instructional information sharing from regulators on a campaign level basis to assist with risk reporting is critical to the success of any enhanced PET or other types of privacy by design for an emergency. Updating privacy laws or creating regulations to address PET use and bare minimum standards may also be helpful in ensuring this area of response requirements and controls is taken into account.

5. Supervision and Enforcement

Generally, the respondents agree that the development of COVID-19 and contact tracing apps are important to develop, and at the same time, innovation in developing them can co-exist with strict privacy compliance and oversight. Most of them also thought that supervision and enforcement should be conducted as usual. There was a reasonably moderate percentage that suggested privacy regulation should be flexible thereby allowing for innovation. Based on experience of the past year, most respondents wanted supervision, outreach and training on Security measures for managing COVID-19 restrictions and data sharing requirements, especially where working from home is necessary. Others indicated they want support in understanding any new or revised guidance on breach reporting during a pandemic, i.e., what is a breach in the new processing environment we find ourselves in, has anything changed, what new factors should be considered, etc.

Lessons Learned:

Developing a better understanding of the impact and transparency about data management and sharing through COVID-19-specific privacy notices may affect how organizations assess the risk and requirement around breach reporting. Regulators can provide guidance about what

issues in such an emergency situation should be clarified to data subjects with respect to data collection and processing during an emergency response period, what regulatory obligations they are subject to, and any other templates for business-critical response controls should be considered.

Conclusions:

While the COVID-19 pandemic continues to be hard fought, personal data remains at risk as tools are developed and gains are made to improve public health and travel at the cost of privacy and potentially security. More information must be collected, some that never existed before or if it did, it was very sensitive, for example medical and health related data that only medical professionals and hospitals had access to. Where more information is collected and processed, risk increases, and additional work must be done to understand new and innovative ways of protecting privacy as well as the risks involved. Ethics becomes even more important, and we as regulators must continue to ask ourselves what we are learning along the way, are we addressing the appropriate issues, and what practically can be done. For future lessons learned surveys, we may consider more nuanced themes, such as:

- ✓ What are the ethical issues around data sharing for the public good (both about sharing and about not sharing data, when is it appropriate, who decides, etc). The concept of "the public good" indicates almost an *imperative* to share data, but it may simply not be feasible or a data subject may strenuously object to it… who wins? What is truly the right thing to do? What if it means retaliation, exclusion, or worse? Could these issues be the result whether the data is shared or not, i.e., the proverbial rock and a hard place? If I share I'm excluded because I have COVID-19, or haven't been vaccinated / don't have an acceptable "standard" record, etc. The GPA COVID-19 Working Group is preparing a resolution on this matter, draft is pending and may be the subject of another, follow up webinar.

- ✓ While data protection and privacy laws and principles are largely about accountability, and making a risk based self-assessment about processing personal data, are there any specific, absolute do's and don'ts for organizations and individuals to follow? Can we as regulators do more to provide clear starting points and specific guidance as subject matter experts calling on people with perhaps less expertise to make some very difficult calls?

- ✓ During a pandemic, does all data sharing simply become high risk processing, such that, at least temporarily, a Data Protection Officer (DPO) or some other role of accountability in any organization, big or small or otherwise, should be appointed? Is this something that becomes part of any national emergency response protocols, required by laws or regulations for example?

The GPA COVID-19 Working Group continues its work to better understand and even get ahead of such issues to help better enable data protection and security at any given time, and for any entity collecting and processing personal data, especially in such precarious times.