Global Privacy Enforcement Network

GPEN Sweep 2020-21

‘Privacy considerations and COVID-19 related solutions and initiatives’

April 2021

Office of the Privacy Commissioner, New Zealand
(Te Mana Mātāpono Matatapu)

Background

In April 2020, the Global Privacy Assembly ("GPA") established the GPA COVID-19 Taskforce to address emerging privacy issues posed by the spread of the virus. In June 2020, the Taskforce conducted a survey to map the most pressing privacy issues facing GPA members. In August and September 2020, a follow-up survey collated relevant experience and best practices for responding to these privacy issues. In October 2020, the GPA published its findings in the Compendium of Best Practices in Response to COVID-19.

Recognizing this valuable reference document for data protection and privacy authorities, health authorities, businesses and other stakeholders involved in the implementation of measures aimed at containing the spread of the COVID-19 disease, the GPEN Committee seek to build on this work with the Sweep.

The aim of the 2020-21 GPEN Sweep is to help us better understand, at the practical level, if and how privacy considerations have been taken into account by the organizations responsible for various COVID-19 solutions and initiatives and what level of engagement data protection agencies ("DPAs") have had with those organizations in their jurisdiction (whether via assessments of contact tracing apps or any other public or private sector initiative). The Sweep explored how the global DPA community engaged with local governments, to identify and understand risks associated with Covid-19 initiatives and made recommendations to improve compliance with privacy and data protection laws. And that, where necessary, (e.g., complaints or continuing risks), enforcement action may be undertaken. We also seek to understand what, if any, enforcement action DPAs might be considering, and what education and outreach activities DPAs conducted.

In previous years, there was a dedicated 'Sweep Week' – a prescribed week in which participating Privacy Enforcement Authorities provide information from their jurisdiction which reflects a full environmental 'sweep' related to a predetermined theme in an effort to assess related privacy practices a prescribed week in which participating Privacy Enforcement Authorities coordinate for a week, in an effort to assess privacy practices related to a predetermined theme. This year, to give participating authorities more time to answer the questions in the Sweep questionnaire, authorities had 3 weeks to complete and return the questionnaire.

This year 20 DPAs from Europe, the Americas, Oceania, Asia and the Middle East participated in the Sweep.

Summary Observations

- All jurisdictions who responded to the questionnaire have been involved in assessing the privacy implications of COVID-19 solutions and initiatives.

- Most jurisdictions have introduced a COVID-19 contact tracing mobile app. Most jurisdictions' contact tracing apps are similar, using Bluetooth technology to alert users if they have been near another app user who tests positive for coronavirus and whether they have visited a venue around the same time as another person who was reported as positive.
- The amount of personal information a contact tracing app collects differs per jurisdiction. For most jurisdictions, the app collects information on name, sex, age range, country of residence, phone number, post code, town, proof of ID, health information, smartphone model, Bluetooth signal strength and data. Most jurisdictions have set clear rules around retention of the data that the app collects.
- Most health authorities carried out a Privacy Impact Assessment (**"PIA"**) for the contact tracing apps. Several risks and mitigations were identified in consultation with local DPAs.
- Most authorities were consulted on local contact tracings app from an early stage and throughout their development. For some jurisdictions, additional privacy protections were incorporated into legislation. Most authorities made recommendations to proposed solutions and initiatives.
- Other solutions and initiatives were also developed in response to COVID-19, such as electronic wristbands, health declarations, protocols to return to work safely, online teaching guidance, national border registers and COVID-19 vaccine registers.
- Most DPAs received privacy complaints about COVID-19 solutions. The number of complaints differs widely among different jurisdictions and not all complaints were investigated. Some DPAs did not initiate any formal investigations but rather addressed issues through informal enforcement measures.
- All DPAs produced educational materials relating to privacy issues and COVID-19. Some DPAs published a dedicated page online to provide specific guidance on good privacy practices in the context of the COVID-19 for individuals, and public and private organisations. Most of these websites include infographics, press releases, blog posts, news, recommendations, and links to other information related to data protection and the pandemic.

COVID-19 initiatives

Most jurisdictions have introduced a COVID-19 contact tracing mobile app and the majority of the participating DPAs have been consulted on local versions.

Most contact tracing mobile apps are similar and use Bluetooth technology to alert app users if they have been near another app user who tests positive for coronavirus and whether they have visited a venue around the same time as another person who is reported as positive.

Some apps also have additional functions including –

- reporting on the risk status in users' areas;
- checking users' symptoms;
- counting down remaining days for self-isolation;
- providing news and updates about national COVID-19 statistics; and
- applying for financial support needed for self-isolating individuals.

Some apps use a QR code check-in application for venues visited by users. This can either be built into the app or in the form of a digital diary, requiring users to scan a QR code poster to keep a personal record of all venues users visited.

In Canada, an individual who tests positive for COVID-19 can obtain a one-time code from provincial health care providers (and in some cases, from a federal portal accessed by provincial health care workers) and enter the code in the app on his or her phone. The app checks a list of codes daily and sends an alert to the phones, that within the previous 14 days, were in proximity to the phone of the individual who tested positive. Alerted individuals can then be tested for COVID-19 and take other appropriate precautionary steps.

Personal information collected by COVID-19 tracing app

The amount of personal information collected by the contact tracing apps differs per jurisdiction. Some DPAs reported that their local contact tracing app does not collect personal information at all because the app uses Bluetooth technology to securely collect and share random IDs with other phones nearby.

Most DPAs indicated that their local apps collect information on name, sex, age range, country of residence, phone number, post code, town, proof of ID, health information, smartphone model, Bluetooth signal strength and data.

Some DPAs indicated that although it is not necessary for a user to register their personal information to use the app, if users are confirmed positive, they may be required to upload their visit records in the app to the local health authority and would be required to provide their personal information, such as name and phone number, as well. Some DPAs said that with encrypted keys, users can be diverted to areas outside the app that may deal in personal information. An example of this is apps that can assist applying for financial support for self-isolating users.

Most DPAs said that the app generates a user ID which is automatically encrypted and stored in the app on the users' phone. Most COVID tracing apps use the Apple and Google Exposure Notification Framework which was developed in accordance with Privacy by Design principles. Apple and Google developed the framework to help governments deal with the COVID-19 pandemic. No personal information is shared with Apple or Google.

In Victoria, Australia, the data is stored in onshore databases, managed by Service Victoria – the Victorian Government's online hub for transacting with government.

This data is encrypted on collection and cannot be used or decrypted by Service Victoria. The data cannot be used for any purpose except contact tracing. If a business, organisation, club or event is identified as having potentially been visited by someone with coronavirus, the Victorian Department of Health's contact tracers make a request to Service Victoria for the digital records, which are then transferred to the Department of Health. The Department of Health can decrypt the data once received. Unless the Department of Health requests a contact tracer's data for coronavirus contact tracing purposes, it is automatically deleted by Service Victoria after 28 days.

For some DPAs, personal information is collected and stored elsewhere (i.e. not on the user's mobile device) such as location data collected as part of the epidemiological investigation of user who tested positive for COVID-19 that is being transferred to a Ministry of Health database subject to and upon users' consent.

One DPA (Canada) indicated that their government notes that personal information is not collected directly by the app. However, there is a collection of IP addresses for cyber security reasons to prevent the app from being disabled by fake exposure notifications. Those IP addresses are kept separate from the server that generates the codes and are not linked to any other information. IP addresses are retained for three months – unless there is an investigation into malicious activity, in which case they are retained for up to two years.

Most jurisdictions have set clear rules around retention of the data that the app collects. For example, Service Victoria will automatically delete the data after 28 days and in New Zealand, digital diary entries are automatically deleted from the phone after 60 days, while Bluetooth keys are deleted after 14 days. Most privacy policies explain that the personal information will be processed as necessary due to the pandemic.

Privacy Impact Assessments

For some jurisdictions, government agencies need to complete a PIA for high-risk privacy projects, however, this is not the case for all jurisdictions. Most DPAs were consulted on a PIA for the local contact tracing app in use.

Some examples of risks that were identified:

- The identification of individuals within the system.
- Automated decision making and associated risks.
- Individuals will not be able to exercise their Chapter 3 rights under the GDPR
- For apps that share information of the infection status with other parties, the risk that the individual will not realise their information will be shared and that the infected individual might be identified.
- Children under 16 might receive a notification.

- The collection of children's data.
- The expansion of phone apps' initial purposes.
- Withdrawal of consent may not be facilitated adequately.
- The lack of balance between the effectiveness of the app and the processing impact.
- Location tracking.

Some other concerns were identified:

- The need to ensure that consent is voluntary and the need for users of the app to understand how their personal information will be handled.
- The need to ensure embeddedness of the 'data minimisation principle' so that the minimum amount of personal information required is collected.
- The need for clarity about retention of personal information collected through the app after the pandemic.

Some examples of mitigations were identified:

- Decentralised systems utilising anonymised keys.
- All data captured in the app is transmitted through encryption and pseudonymisation in a way that makes it hard to connect the data to the specific user. However, it is accepted that there is no such thing as zero risk of the re-identification of de-identified data. Most DPAs found that considering the security and other safeguards adopted, the risk of re-identification is low.
- The incorporation of the purpose limitation principle (e.g., contact tracing app is only to be used for contact tracing purposes).
- Users are provided with detailed information on the functions and risks of the contact tracing app.
- For apps that notify others of the infection status of the user, consent should be sought from the user both before activating the application and before others would be notified that they have been in the vicinity of the user who got infected.
- For the app to be developed in line with European Data Protection Board guidelines on privacy by design and default.
- After the pandemic is over, all data from the app should be deleted as soon as reasonably possible, and users will be informed of this.
- Having an external advisory panel provide expert advice on implementation of the app.

Stages of involvement

Most authorities were consulted on their local contact tracing app from an early stage and throughout its development.

In the UK, the authority produced an expectation document for developers to refer to as they considered the data protection implications of the design choices they were making as they built the country's contact tracing app.

Most jurisdictions' health authorities set out some form of PIA and consulted on these with their local authority. Most authorities continue to be engaged with the development of local contact tracing apps in some form of governance function, providing guidance on the PIAs and privacy notices as new functions are added.

For some jurisdictions, additional privacy protections were incorporated into legislation. For example, the OAIC in Australia recommended for privacy safeguards to be enshrined in legislation to engender public trust and confidence in the use of the Australian Government's COVIDSafe contact tracing app and promote privacy by design principles. These recommendations were accepted by the Australian Government and additional protections were incorporated into legislation. Similarly, the Catalan authority was consulted on legal provisions regarding personal information sharing between their Health Department and other departments, such as the Social Affairs and Families Department, the Education Department, local authorities, and between hospitals.

A European DPA imposed a temporary ban on the processing of data in connection with the contact app due to non-compliance with the GDPR. Based on the suggested amendments, the app was updated, and a new version was released.

Recommendations to amend solutions/initiatives

Most authorities made recommendations to the proposed solutions/initiatives. These recommendations included:

- explaining to individuals the purposes for which the information is collected and how it will be used or disclosed to achieve these purposes;
- limiting the purpose to COVID-19 related matters or making reference to the potential use or disclosure for secondary purposes;
- committing to deleting the data when no longer required for the COVID-related purposes;
- engaging with the local DPA when the time to dismantle the app comes and making the decommissioning plans public;
- carrying out a PIA;
- minimising the collection of personal information;
- using appropriate security measures for the transfer and storage of personal information;
- better enabling the exercise of data subject rights;
- locally storing all data (on mobile devices) instead of uploading to a central database; and
- encouraging greater transparency around data sharing.

Some apps were based on using location data instead of Bluetooth data only. The European Data Protection Board found that the use of location data in contact tracing is unnecessary and recommended the use of Bluetooth data only.

One authority recommended that the government closely monitor and evaluate the app's effectiveness during its use to meet the test for necessity and proportionality.

Some authorities also provided guidance and advice in relation to the Bilateral Agreements between federal, provincial, and territorial governments on the collection, use and disclosure of the tracing app's data.

Other solutions and initiatives

This section discusses some of the other solutions and initiatives that jurisdictions have developed in response to COVID-19.

Electronic wristband

Hong Kong introduced the use of an electronic wristband (with QR code), paired with the 'StayHomeSafe' mobile app for inbound travellers who are subject to compulsory home quarantine orders. Its aim is to detect non-compliance by employing 'geo-fencing technology'; an alert will be triggered if the person has moved away from the vicinity of their quarantine dwelling. The mobile app collects electronic signals in the surrounding environment (e.g., Wi-Fi, mobile networks, GPS signals) together with the Bluetooth signal of the electronic wristband, and their respective strengths. Data analyses of signal changes are conducted for continuous monitoring during the quarantine period to assess if the quarantined person is staying at the designated place in accordance with the quarantine order. The authority will receive an alert if the app loses its connection with the wristband or detects significant change in the environmental signals. Spot checks and surprise video calls are made to the person under quarantine; the app also randomly requests the quarantined person to scan the QR code on his wristband as a spot check measure.

Upon installation of the app, the user is required to link the app to the wrist band (by scanning the QR code on the band); and to register his phone number which has been provided under the quarantine order. Thereby, a linkage is created between the mobile app and the identity of the user. The detection and analysis of environmental signals by the app, during its operation, do not involve collection of personal information. The app does not read any information in the user's smartphone.

The DPA recommended the following good practices on the use of digital contact tracing measures:

- Adherence to the principles of necessity and proportionality in data collection and use;

- The monitoring measures should be time-bound and continue only for as long as is necessary to address the COVID-19 pandemic; and
- Transparency around data transfers to other authorised parties.

Health declaration

In Israel, employers, business owners and service providers have been legally required to take measures to ensure that only individuals who do not have COVID-19 are granted access to their premises. One of the measures that had been implemented was a requirement to obtain a health declaration from individuals who wish to enter the premises. As part of this health declaration, the relevant individuals must provide personal information regarding their health (e.g., body temperature within the normal range, no indication of other COVID-19 symptoms, etc.), and declare that they have not been in contact with any confirmed COVID-19 carrier in the 14 days preceding the declaration. The Israeli DPA published guidelines to clarify what information may be collected in this regard (i.e., types of information that would be considered necessary for the purpose), and to what purposes its use must be limited.

National Return to Work Safely Protocol

In Ireland, the National Return to Work Safely Protocol is a series of initiatives for employers bringing people back to work post-lockdown. Principally it involves a pre-return-to-work health declaration form and the collection of group contact details for contact tracing purposes in the event of an outbreak. The pre-return-to-work form collects name and COVID-19 symptom details, the Small Group Contact Tracing log contains name and contact details for employees. It is the responsibility of each employer to handle the provision of privacy information in the scheme, however following intervention by the DPA wider guidance was published.

COVID-19 Vaccine registers

Many jurisdictions created COVID-19 vaccine register. A COVID-19 vaccine register collects personal information such as name, place of birth, date of birth, gender, email addresses, phone number, Individual Registration Number, and address. The initiative demonstrates how personal information is used and disclosed. The personal information collected will be used to carry out the registration of the individuals to be vaccinated so that the health authority can organise the distribution of doses, as well as scheduling appointments and sending notifications.

Exemption from notifications

In Macao, SAR China, the DPA issued an Exemption from Notification 01/2020 to exempt data controllers from notification obligations to notify their DPA regarding the collection of the data subject's health declaration. However, for a transfer of data outside Macao using an overseas server for the storage of data the data controller would notify the DPA by submitting a simplified notification form.

The health declaration includes the following personal information: name, ID number, phone numbers, any related symptoms, cities, or jurisdictions visited in the past 14 days.

Online teaching guidance

The Italian DPA worked together with their Ministry of Education on the issue of data processing of pupils and teachers by software applications such as the electronic school register or distance learning practices. The DPA provided guidance on data protection and online teaching, provided FAQs on going back to school and worked on a national platform development project aimed at offering e-learning, digital education, and electronic school register tools.

National Border Register

The New Zealand borders are closed to almost all travellers. Arrivals are required to undergo either managed isolation or quarantine for at least 14 days. The National Border Register enables records of individuals entering managed isolation to be recorded. It replaced manual record keeping about individuals coming across the border and matches these individuals to a National Health Index number (a unique number that is assigned to each person who receives healthcare in New Zealand). The New Zealand OPC was consulted on the PIA of this register.

Enforcement and complaints

Most authorities received privacy complaints about local COVID-19 solutions. The number of complaints differs widely per jurisdiction – some have not received any complaints, while others received more than 350 complaints. Not all complaints were investigated.

Some DPAs did not initiate any formal investigations but addressed issues through informal enforcement measures, for example, scrutinising COVID-19 related data transfers, reviewing epidemiological investigation processes and engaging with food and beverage outlets that misuse contact tracing information.

Here are some examples of the complaints made and investigations that were carried out:

In Ontario, Canada, the Office of the Information and Privacy Commissioner opened an investigation into a potentially disproportionate number of inquiries by several police services in Ontario into the COVID-19 first responder portal. This portal contains confirmed positive test results for individuals who have undergone a COVID-19 test. An individual who is included is never removed, even if they have subsequently recovered. The investigation is ongoing, but police access to the portal and database has ended.

Similarly, in New Zealand, OPC received complaints from individuals indicating that the Police vetting service received health information about patients who had tested positive for COVID-19. OPC contacted Police to ask about this practice, who confirmed this information was being entered into the National Intelligence Application and was therefore available to all officers with access to that system. The Privacy Commissioner undertook an inquiry into whether:

- the Ministry of Health's disclosure of COVID-19 patient information to emergency services was compliant with the information privacy principles and rules of the Health Information Privacy Code 1994 ("the Code");
- the disclosure infringes or may infringe individual privacy;
- whether Police's access to and use of COVID-19 patient information was compliant with the privacy principles and rules of the Code; and
- whether it infringes or may infringe individual privacy.

In Italy, the DPA received several complaints regarding the processing by healthcare facilities of personal information as part of the management of healthcare emergencies. In addition, they investigated the processing of data carried out through apps promoted by regions and other public entities in relation to the pandemic. As a result, the DPA initiated a preliminary procedure against a regional app aimed at drawing a map of the contagion based on the completion of a daily questionnaire by users.

Italy also received several complaints about data processing by schools and universities, specifically regarding:

- online learning;
- the lawfulness of tracking body temperature of students;
- the lawfulness of recording online lessons;
- the lawfulness of creating pupils and teachers accounts to access online learning services and platform;
- health status self-declaration of pupils/students/relatives in order to return to school;
- the type of data of pupils, students and relatives collected by schools in the context of COVID-19 prevention;
- the notification of schools about data subjects' COVID-19 test results;
- data processing in the context of COVID-19 screening in the school environment; and
- software used during university oral and written tests.

In Mexico, public servants were taking photographs of vaccinated people's faces along with their identification documents. This was confirmed by an on-site investigation by the DPA. As a result, the DPA initiated ex officio a preliminary investigation on the protection of personal information.

The Federal Trade Commission in the US has taken a range of enforcement actions in response to the pandemic (https://www.ftc.gov/coronavirus/enforcement) in respect of private sector organisations. Issues that were addressed included financial scams, promises of fast delivery of PPE, and unsubstantiated treatment and prevention claims.

In Australia, the OAIC was granted additional functions and powers in relation to COVIDSafe app data under Part VIIIA of the Privacy Act 1988. Part VIIIA enhances the Australian Information Commissioner and Privacy Commissioner's role in dealing with eligible data breaches and conducting assessments and investigations in relation to the app and the app data. Part VIIIA also requires COVIDSafe app data is stored onshore and not disclosed outside of Australia. As part of this mandate, the OAIC established the COVIDSafe Assessment Program, which follows the 'information lifecycle' of personal information collected by the app.

Between May to November 2020, the OAIC commenced four assessments[1]:

- Assessment 1 – Access controls applied to the National COVIDSafe Data Store by the data store administrator, the Digital Transformation Agency
- Assessment 2 – Access controls applied to the use of COVID app data by state and territory health authorities
- Assessment 3 – Functionality of COVIDSafe against specified privacy protections set out under the COVIDSafe privacy policy and collection notices and against the requirements of the Privacy Act
- Assessment 4 – Compliance of the data store administrator with data handling, retention and deletion requirements under the Privacy Act.

Educational materials

All DPAs produced educational materials relating to privacy protection issues and COVID-19. Some DPAs published a dedicated page online to provide specific guidance on good privacy practices in the context of the COVID-19 for individuals, government agencies and organisations. Most of these pages/websites include infographics, press releases, blog posts, news, recommendations, and links to other information related to data protection and the pandemic.

For example, New Zealand created educational material on the following:

- Privacy issues relating to COVID-19.
- Contact tracing.
- Hospitality businesses and event organisers.
- Employers and employees and COVID-19.

[1] Results can be found here - https://www.oaic.gov.au/updates/news-and-media/oaic-issues-first-6-month-covidsafe-privacy-report/

- Landlords and tenants during the pandemic.
- Information for healthcare professionals.

Some examples of these pages/websites are:

- New Zealand - https://privacy.org.nz/resources-2/privacy-and-covid-19/
- Australia - https://www.oaic.gov.au/updates/covid-19-advice-and-guidance
- Norway - https://www.datatilsynet.no/personvern-pa-ulike-omrader/korona/
- Mexico - https://micrositios.inai.org.mx/covid-19/
- United Kingdom - https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/

In Gibraltar, the Deputy Head of the Information Rights Division of the Gibraltar Regulatory Authority ("GRA"), was interviewed by the Gibraltar Broadcasting Cooperation ("GBC") as the public service broadcaster. During the interview, which focussed on the topic of data protection in the current COVID-19 climate,[2] the GRA advised about the added strain experienced by many businesses adopting remote working models and discussed some of the data protection concerns presented as a result. Matters discussed included, amongst others: the potential for personal data to be compromised; the increased risk of cybercrime due to increased use of online resources; and the need to ensure compliance with the principles for processing personal data as provided within the GDPR. In particular, the GRA reiterated the need to limit the processing of personal data to what is absolutely necessary.

In a second television and radio interview, GBC featured the Assistant Information Commissioner, who focused on ongoing contact tracing efforts[3] in Gibraltar. In this interview, the GRA reminded establishments about the importance of processing the personal data collected as part of such efforts in compliance with the Government's regulations and data protection legislation.

The Federal Trade Commission in the US (FTC) has a dedicated page which (https://www.ftc.gov/coronavirus/scams-consumer-advice) addresses privacy and security related topics like contact tracing scams, government imposter scams, online learning tips and online working tips for consumers. The FTC has also provided materials on financial, work-from-home, treatment, and PPE-related scams.

Australia created an online step-by-step PIA tool to help guide organisations and agencies through their PIA process for remote working arrangements. This tool can be found here - https://www.oaic.gov.au/privacy/guidance-and-advice/assessing-privacy-risks-in-changed-working-environments-privacy-impact-assessments/

[2] https://www.gbc.gi/news/gra-advises-businesses-preserve-data-protection-lockdown-leads-increase-remote-working
[3] https://www.gbc.gi/news/gra-personal-data-collected-contact-tracing-must-comply-regulations.

Israel produced guidance on the privacy considerations associated with the use of drones in response to the Israeli police's request to use drones as part of their effort to contain the pandemic and enforce mandatory quarantine obligations.

Most DPAs published guidance for employers and employees on protecting personal information while Working-From-Home, data security regarding video conferencing, data processing for clinical trials and medical research, and, vaccination data.

Most DPAs produced guidance on one or more of the following subjects:

- The use of teleconferencing tools and the expectations for technology companies to secure such tools and provide information on how individuals can protect their privacy and personal information while connecting virtually;
- Best practices guidance on remote exams for academic institutions;
- Digital tracing in times of this pandemic;
- Information on vaccinated individuals;
- Guidance for schools on the collection and use of personal information for teachers, staff and students during the pandemic;
- Processing of customer data for contact tracing purposes; and
- PIAs during a public health emergency; virtual care to patients.

Conclusions

Overall, governments and their health authorities around the world have taken into account privacy considerations in implementing COVID-19 initiatives. While some jurisdictions' DPAs found it necessary to carry out complaint-led and ex-officio investigatory action into COVID-19 initiatives, local DPAs were well engaged in initiatives.