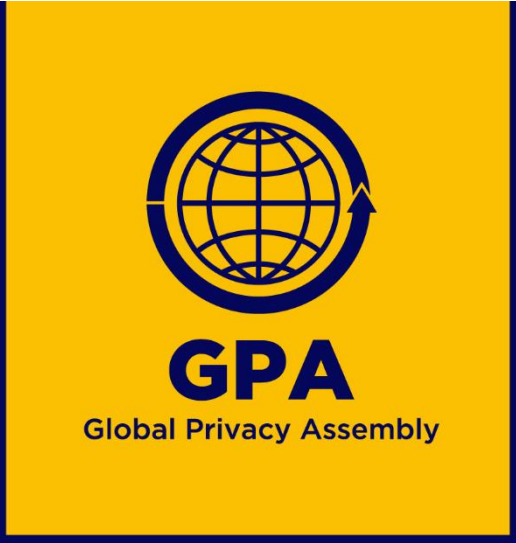


GPA COVID-19 Taskforce: Compendium of Best Practices in Response to COVID-19

October 2020

globalprivacyassembly.org

Table of Content

Executive Summary

GPA COVID-19 Taskforce
Compendium of Best Practices in Response to COVID-19

1. First appearing at the end of December 2019, COVID-19 quickly developed into a global health crisis. The World Health Organisation ("**WHO**") declared COVID-19 a Public Health Emergency of International Concern on 30 January 2020. On 11 March 2020, the WHO declared the outbreak of the COVID-19 disease a pandemic. As at 4 October 2020, there were over 34.8 million COVID-19 cases and over 1 million deaths reported to the WHO from around the globe.

2. Governments and public authorities have been taking a number of measures to contain the spread of the disease, such as track and trace measures to map out infections, lock down measures (including across borders), and implementing a variety of social distancing rules aimed at reducing close social interaction, including 'work from home' schemes. The implementation of these measures resulted in having an impact at economic level while track and trace efforts, including through digital solutions, and the increased use of platforms for remote working and learning translated into higher privacy risks for individuals' personal data.

3. Recognising the privacy and data protection challenges posed in the context of the COVID-19 pandemic, the Executive Committee of the Global Privacy Assembly ("**GPA**") agreed in April 2020 to establish the GPA COVID-19 Taskforce to address the emerging privacy issues posed by the spread of the virus. One of the planned deliverables of the Taskforce was the collection of relevant experience and best privacy practices to deal with the privacy issues arising from the measures being adopted in response to the spread of the virus. This resulted in this **Compendium of Best Practices in Response to COVID-19**. The Compendium draws from the responses to a **survey conducted in August and September 2020** and collates the relevant **experience and best practices of 32 GPA members and observers.** It covers the following five topics:

   (1) Contact tracing and location tracking;
   (2) Sharing of health data with health authorities and institutions;
   (3) Sharing of health data with law enforcement agencies;
   (4) Sharing of health data with charitable or other similar organisations; and
   (5) Handling of employee data in work-from-home / return-to-work situations.

4. These topics were chosen because they were identified as the most pressing issues by GPA members according to the findings of another survey conducted by the GPA COVID-19 Taskforce in June 2020.

5. The geographical distribution of the responses received for the current survey on the aforementioned five topics is as follows:

Geographic distribution of responses	
Africa	2
Asia	3
Europe	21
North America	3
Oceania	3
Total	**32**

6. The following is a digest of the responses of these 32 members and observers of GPA on each of the five topics.

(1) Contact tracing and location tracking

7. At a media briefing on COVID-19 in March 2020, the Director-General of the WHO, Dr Tedros Adhanom Ghebreyesus, said, "*You cannot fight a fire blindfolded. And we cannot stop this pandemic if we don't know who is infected.*[1]" This is one of the reasons which made contact tracing and / or location tracking common measures across jurisdictions for speedily identifying the close contacts of infected persons with a view to containing the spread of COVID-19.

8. Among the 32 data protection authorities (hereafter "**DPAs**[2]") which provided responses to the survey, **27 DPAs (84%) stated their jurisdictions had used or would soon use digital technology for supporting manual contact tracing measures to contain the spread of the COVID-19 pandemic. Majority (23 out of 32, or 72%) of the jurisdictions used contact tracing apps.** Other digital technology included those for enforcing quarantine and for assessing the health status of individuals.

[1] Alfred Ng, *Coronavirus pandemic changes how your privacy is protected*, CNET (21 March 2020): https://www.cnet.com/news/coronavirus-pandemic-changes-how-your-privacy-is-protected/

[2] The term "data protection authority" or "DPA" is adopted in this Compendium to refer to a GPA member or observer for the sake of convenience, although some GPA members and observers may not recognise themselves as DPAs.

9. Of the 23 jurisdictions that used contact tracing apps, there were **19 jurisdictions which had their own apps**[3]. Among these 19 jurisdictions with contact tracing apps, **16 (84%) used Bluetooth technology** for digital contact tracing. Among the 16 jurisdictions that used Bluetooth technology, **10 of them (63%) were based on the exposure notification API jointly developed by two tech giants**. While contact tracing and exposure notification do not necessarily involve tracking of physical locations of individuals, **8 DPAs (out of 32, or 25%) stated that their jurisdictions had also implemented location tracking by using GPS or data of mobile operators**.

Use of digital technology to combat COVID-19	
No. of jurisdictions that used digital technology	**27** out of 32 (84%)
No. of jurisdictions that used contact tracing apps	**23** out of 32 (72%) (**19** jurisdictions had their own apps[4])
No. of jurisdictions with contact tracing apps based on Bluetooth technology	**16** out of 19 (84%)
No. of jurisdictions with contact tracing apps based on the API of the two tech giants	**10** out of 16 (63%)
No. of jurisdictions using location tracking	**8** out of 32 (25%)

10. The level of privacy intrusiveness of different digital measures varies. The exposure notification jointly developed by the two tech giants is considered more privacy friendly as it does not involve location tracking or aggregation of contact information in a central database. By contrast, location tracking using GPS or data of mobile operators is considered more privacy intrusive because this method may enable the relevant authorities to track the everyday movements of individuals.

Constructive engagement by DPAs

11. Due to the privacy concerns arising from the use of digital measures, engagement with DPAs in the process was high. Among the 32 jurisdictions which provided responses to the survey, **22 jurisdictions (69%) consulted their DPAs** with respect to data protection / privacy impact assessments and other general privacy issues in the development and deployment of digital measures.

[3] Some jurisdictions used the contact tracing apps of others. Liechtenstein recommended individuals to use the contact tracing app of Switzerland. In Australia and Canada, the same contact tracing apps are used across the countries. Hence, the contract tracing apps reported by the federal DPAs of Australia and Canada were the same as those reported by their provincial DPAs, i.e. Victoria in Australia; Newfoundland and Labrador and Québec in Canada.

[4] See footnote 2.

The DPAs generally considered that their engagement with the relevant authorities had been constructive. A few DPAs (such as those of Finland, Japan, the Netherlands, Switzerland and the UK) even played an active role by participating in special taskforce or committees for the developing of contact tracing apps, or by direct discussion with the app developers.

Legislative amendments

12. Some DPAs stated that legislation had been introduced or amended in their jurisdictions to facilitate contact tracing. According to the responses received, some of the laws aim at **addressing the privacy concerns** arising from the implementation of contact tracing solutions and at **strengthening personal data protection safeguards around their use**. For example, in Australia, amendments to the Privacy Act 1988 were made to limit the use of COVIDSafe app data for contact tracing purpose only and to introduce a new criminal offence for coercing or requiring someone to download or use the COVIDSafe app, among other protection for personal data privacy. In the Netherlands, legislation was being discussed in the Parliament to, among others, prohibit anyone from making the use of notification apps or other comparable digital technology as a pre-condition for access to a building, for work or for use of a service, etc. In addition, in Quebec, a bill aimed at improving the current provincial laws was introduced last June by the government of Quebec.

13. By contrast, some jurisdictions amended their laws to **facilitate the use of data for contact tracing** or for enforcing mandatory quarantine. For example, in Slovakia, special legislative measures have been enacted to create a legal basis for the processing of personal data by the contact tracing app used in the country. In Bulgaria, legislative amendments were made to obligate mobile operators and internet service providers to collect location data of a person violating a confinement order.

Best practices

14. From the responses received, the best practices which have emerged in different jurisdictions to address the privacy concerns arising from digital contact tracing are as follows.

    a. One of the most common practices was conducting **data protection / privacy impact assessments** before rolling out the contact tracing apps to ensure **Privacy by Design**.

b. Almost all contact tracing apps in use (except those for enforcing quarantine order) were **voluntary**.

c. Various **data minimisation** techniques were adopted by the contact tracing apps, 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).

d. Various measures were also adopted by different jurisdictions to **increase transparency and enhance public trust**, such as (i) publishing privacy policies of the contact tracing apps (e.g. Japan), (ii) opening up the source code of the apps (e.g. the Netherlands), (iii) informing the users when their data is deleted (e.g. Australia), and (iv) chartering the DPAs or oversight committees to review the operation of the apps (e.g. Canada, Germany and the UK).

e. Some jurisdictions **spelled out the exact retention periods** for the data collected by contact tracing apps, although retention periods across jurisdictions varied greatly, from 14 days to 3 years. The more common retention period is from 14 to 30 days after collection.

f. Some jurisdictions pledged that the contact tracing apps would be **scrapped when the COVID-19 pandemic is over**.

15. Given the privacy concerns and the large of amount of personal data involved, the use of contact tracing apps warrants continued monitoring by DPAs. A **majority (22, i.e. 69%) of the DPAs** which responded to the survey indicated that they had **issued guidelines or opinions** relating to the use of digital contact tracing.

16. As we observed from the responses of some DPAs, it would also be preferable to **continuously assess the efficacy of contact tracing apps**, which is a key factor when assessing whether the collection and processing of personal data by the contact tracing apps is proportionate. A contact tracing app with low efficacy may not be justified to collect data from a large amount of people, even if good data protection practices are in place.

(2) Sharing of health data with health authorities and institutions

Legal requirements

17. During the current COVID-19 pandemic, public health authorities need sufficient information (e.g. identities of the infected, the places they visited and data about whom they interacted with) in order to contain the spread of the virus. According to the findings of the survey, **most of the DPAs (25 out of 32, i.e. 78%)** stated that there were **laws or regulations in place** in their jurisdictions that require or allow sharing of health data with public health authorities.

18. Among the relevant laws and regulations reported by the 25 DPAs, some of them were **specifically made or amended in response to COVID-19** (e.g. Australia and Hong Kong).

Retention of data by health authorities

19. Retention periods of the health data collected by health authorities vary across jurisdictions. For example, data related to contact tracing collected by health authorities should be **deleted after 21 days and 60 days** in Jersey and Belgium respectively. Some jurisdictions adopted a more flexible and principle-based approach, such as allowing health data to be retained as long as **there is a reasonable purpose** (e.g. Andorra) or **if it is necessary for contact tracing** (e.g. the Philippines). Some jurisdictions have legislation in place prescribing the retention period of health data in general. For example, in the Netherlands, health data can be retained by municipal health authorities for **up to 5 years**. In New Zealand, regulations require that health records shall be kept for **a minimum of 10 years**.

20. Some DPAs stated that health data may be retained for **research purpose** if the data is **anonymised or pseudonymised** (e.g. Albania, Bulgaria, Germany, Hong Kong, Jersey and Luxembourg).

Roles of DPAs and best practices

21. DPAs have been taking an active role in monitoring the sharing arrangements of health data. **Eleven out of 32 DPAs (34%)** stated that they had **issued guidance, opinions or advice** on the processing of health data during the COVID-19 pandemic (e.g. Albania, Andorra, Belgium, Georgia, Hong Kong, the Philippines and the UK).

22. Some DPAs had a deeper involvement in data sharing arrangements. For example, in Canada, there is a policy requirement to inform the Office of the Privacy Commissioner of any planned initiatives that may have an impact on the privacy of Canadians, usually together with submitting the privacy impact assessments. In San Marino, the opinion of the Data Protection Authority has to be sought before a data sharing arrangement was implemented.

23. In New Zealand, the Office of the Privacy Commissioner initiated an own-motion inquiry into the distribution of COVID-19 patient information by the Ministry of Health. A range of advice was provided to health authorities and institutions, such as-

    a. notifying patients about the collection purposes and intended transferees of their information;
    b. considering obtaining patients' consent before disclosure of their health data;
    c. disclosing only the necessary information;
    d. ensuring data recipients were aware of the privacy risk and were taking actions to mitigate them; and
    e. developing a memorandum of understanding to establish clear expectations about the use of patient information by the data recipients.

24. Other best practices for the sharing of health data which emerged from the responses to the survey include:

    a. conducting data protection / privacy impact assessment as well as an ethical evaluation;
    b. consulting DPAs beforehand;
    c. defining the purposes of data sharing;
    d. defining the specific kinds of personal data to be shared;
    e. sharing anonymised / pseudonymised / de-identified data instead of personal data, where possible;
    f. entering into written data sharing agreements;
    g. limiting secondary uses and onward transfer of the health data;
    h. adopting adequate and proportionate data security measures;
    i. being clear, open and honest about the sharing of health data;
    j. keeping proper records about the data sharing arrangements; and
    k. destroying the data after the sharing purposes are fulfilled.

(3) Sharing of health data with law enforcement agencies

25. Sharing of data with law enforcement agencies may not be as forthcoming as that with public health authorities due to their different roles and functions. That said, according to the findings of the survey, it was not uncommon for the data to be shared with law enforcement agencies for the purpose of combating the spread of COVID-19. **Twelve out of 32 DPAs (37%) stated that there were laws, regulations or other arrangements in their jurisdictions that enable such sharing**.

26. The sharing may be made under existing legal frameworks (e.g. Albania, Canada, Germany, Japan, Hong Kong, Newfoundland and Labrador, Slovakia), pursuant to the **exemptions under personal data protection laws** and / or the **general investigation powers of the law enforcement agencies**. The sharing may also be based on new regulations / arrangements being implemented during the COVID-19 pandemic (e.g. Georgia and the Philippines). The most common reason for sharing data with law enforcement agencies was to **enforce quarantine orders** (e.g. Georgia, Newfoundland and Labrador, and Slovakia).

27. By contrast, in Australia, the amendments to the Privacy Act 1988 passed in 2020 specifically **prohibit the sharing of COVIDSafe app data for law enforcement purpose**, unless the purpose of sharing relates to enforcement of the privacy protection enshrined in the Privacy Act 1988.

28. As regards the best practice for data sharing with law enforcement agencies, they are similar to those for sharing data with public health authorities as mentioned before.

(4) Sharing of health data with charitable or other similar organisations

29. The arrangement of sharing health data with charities was **uncommon** according to the findings of the survey. **Only three out of 32 (9%) DPAs** which responded to this question stated that such arrangements were in place in their jurisdictions (i.e. Burkina Faso, Finland and the UK). The purpose of such data sharing was mainly to allow the **provision of assistance and daily essentials** to COVID-19 infected persons in need.

30. Some DPAs (e.g. Canada and Japan) stated that their personal data protection laws might allow such sharing by **exemptions**, such as public interest exemption or the need to protect lives.

(5) Handling of employee data in work-from-home / return-to-work situations

31. The outbreak of the COVID-19 pandemic has brought new challenges to employers and employees with regard to data security, as well as and personal data and privacy protection. Under work-from-home arrangements, files and data may be transferred from the secure environment of the employers to employees' homes or personal devices, increasing the risk of data leakage. When employees return to workplaces, employers may be required to collect employees' health data and travel histories in order to assess the risk of COVID-19 infection, which gives rise to privacy concerns.

32. The fast-paced spread of the pandemic and rapid changes in the curve of infections has meant that often decisions about new ways of working were limited and had to be made quickly. Both employers and employees may also be unfamiliar with new ways of working. As a result, data security risks may increase.

33. According to the findings of the survey, **nine out of the 32 DPAs (28%) stated that they had received complaints or enquiries** relating to work-from-home or return-to-work situations during the current COVID-19 pandemic. Some of the cases concerned collection of employees' health data (e.g. temperature measurements). Further, **21 out of the 32 DPAs (66%) stated that they had issued guidance or advice** on work-from-home or return-to-work situations.

34. As a general observation from the responses of the 32 DPAs, despite the challenges faced by employers in the time of COVID-19 pandemic, the general data protection principles were expected to continue to apply in the handling of personal data by employers. Indeed, given the higher data security and privacy risk, employers and employees should be more vigilant.

Work-from-home

35. According to the survey results, DPAs identified the following **data security and data privacy concerns** with respect to work-from-home situations:

    a. the rapid uptake of video conferencing apps;
    b. difficulty in ensuring confidentiality of employers' data being transferred to employees;
    c. difficulty in protecting employees' privacy with regard to the private information stored in employees' personal devices used for work or corporate devices;

d. exposure of employees' private and family lives;
e. security of the ICT networks and devices (in particular employees' personal devices);
f. difficulty in the handling of paper files;
g. difficulty in ensuring that data processors adhere to the same data protection standards; and
h. increased risk of data breach due to deviation from standard processes.

36. The survey findings show that the following **best practices** were identified by respondents to address the above data security and privacy concerns:

<u>For employers</u>

a. conducting risk assessments, in particular considering how the changes in the work arrangements may impact data security and personal data privacy;
b. developing internal policies and convey them clearly to employees;
c. ensuring reasonable steps are in place to safeguard data security;
d. using two-factor authentication for access to companies' networks and requiring changing passwords regularly;
e. allowing employees access to data only on a need-to-know basis;
f. logging remote access to companies' network and reviewing the logs regularly where possible;
g. keeping a register of files transferred from and returned to office premises;
h. ensuring appropriate control (such as using agreements) over how external service providers will handle the data entrusted to them;
i. raising employees' awareness on phishing and social engineering attacks (in particular those using COVID-19 related messages); and
j. requiring employees to report data breaches immediately.

<u>For employees</u>

a. following employers policies, procedures and guidance;
b. using companies' devices rather than personal devices for work, where possible;
c. using only hardware and software approved by employers;
d. ensuring security of personal devices if it would be used for work;
e. keeping software up to date;
f. using strong passwords, and changing them regularly;
g. avoiding working in public places;
h. doing business calls in locked rooms;

i. using secure Wi-Fi networks or ethernet for work;
j. using visual protection sheets on the monitors of electronic devices, where necessary;
k. turning off microphones and cameras when not in use;
l. transferring physical files securely, such as using cases with locks;
m. keeping work files at home securely, such as locking up the paper files and electronic devices after work or when they are not in use, and encrypting electronic files;
n. not mixing employers' data with employees' own personal data;
o. not disposing of work-related documents at home;
p. being vigilant about opening web links and attachments in emails or other messages; and
q. notifying employers immediately in the event of data breach.

Return to work

37. As regards return-to-work arrangements under COVID-19, in their responses to the survey, DPAs identified the following **concerns**:

a. proportionality regarding the collection of personal data from employees to combat the spread of the COVID-19 diseases, in particular sensitive health data;
b. security of personal data collected from employees;
c. allowable use and disclosure of employees' personal data; and
d. retention period of employees' personal data (including sensitive health data).

38. According to the survey findings, DPAs provided the following **advice to employers** with regards to the handling of employees' personal data:

a. collecting, using and disclosing only the minimum amount of personal data reasonably necessary to prevent or manage the spread of the COVID-19 disease, or for contact tracing purpose;
b. adopting self-reporting mechanisms in data collection, rather than mandatory collection;
c. avoiding using devices with facial recognition or image recording function for temperature check;
d. informing employees how their personal data will be handled, including whether and how their personal data would be disclosed in responding to potential or confirmed cases of COVID-19;

e. ensuring reasonable steps are in place to safeguard the security of personal data;
f. disclosing employees' personal data only when necessary. For example, while it may be necessary to disclose personal data of employees infected with COVID-19 to public health authorities, disclosing the identity of the employees to other parties is considered unnecessary and disproportionate in most cases;
g. destroying personal data once it is not reasonably necessary for contact tracing or related purposes, except where there are legal obligations to retain; and
h. reviewing COVID-19 related initiatives regularly and considering whether they would still be necessary in light of the latest circumstances.

Closing remarks

39. The COVID-19 pandemic may persist for some time. This means that the implementation of the above measures – contact tracing, including via digital solutions, the sharing of data, working from home and other measures – may be required for as long as necessary till a vaccine is found. This Compendium collates the relevant experiences and best privacy practices in the context of the COVID-19 pandemic from across the GPA community. We hope it will provide a valuable reference document for data protection and privacy authorities as well as for health authorities, businesses and other stakeholders involved in the implementation of measures aimed at containing the spread of the COVID-19 disease with the view of encouraging them to place personal data protection and privacy at the forefront of any COVID-19 response programme.

Office of the Privacy Commissioner for Personal Data, Hong Kong, China
October 2020

Experience and Best Practices of GPA Members

Albania - Information and Data Protection Commissioner (IDP)

1. Contact tracing and location tracking

There is no contact tracing or location tracking measure aimed at containing the spread of COVID-19 under IDP jurisdiction.

Aiming at playing a proactive approach, the IDP Commissioner has developed guidelines to assist public and private controllers if they use tracking apps and transmit data via electronic communication networks.

In order to assist in the course of processing citizens' health data in order to prevent the spread of the pandemic, the Office of the Commissioner has published: *Guidelines for the protection of personal data in the context of measures against COVID-19; Guidelines to the processing of personal data in specific sectors in the context of the measures against COVID-19; Guidelines for the processing of personal data according to the Protocols of Hygienic-Sanitary Measures COVID-19*, as well as a paper on the Statement of the Executive Committee of the Global Privacy Assembly (GPA) on the coronavirus pandemic COVID-19 which are published on the official website of the Office of the Commissioner www.idp.al.https://www.idp.al/udhezime-ne-kuader-te-covid-19/.

2. Sharing of health data with health authorities and institutions

The IDP has published on its official website guidelines on legitimate processing of health-related data, technical and organizational measures, processing of health related personal data in specific sectors, according to protocols of hygienic-sanitary measures COVID-19. By means of these guidelines, the IDP addresses technical and organizational measures which should be taken into account by the controllers when they process health data, disclose the data, etc., in the context of the measures taken against COVID-19.

Health-related data which are collected by the controllers in the context of implementing Protocols of hygienic-sanitary measures against COVID-19, consist on the following categories (but not limited to): name, surname, address, workplace, travel details, potential contacts, other associated health issues, which along with COVID-19 may have serious consequences for the life of individuals, etc.

Personal data and health-related data must not be made public. However, their disclosure may only be made with authorized law enforcement institutions for such purpose, under the law and the respective protocols and on appropriate safeguards.
In the context of the measures against the global pandemic caused by COVID-19, bodies engaged in the fight against COVID-19 may have mandatory or necessary needs to carry out international data transfers with various countries and/or international organizations, for statistical, scientific purposes and/or for more specialized analysis purposes. In this context, the Office of the Commissioner considers that the above-mentioned controllers should act in accordance with the provisions of Articles 8 and 9 of the Law on Personal Data Protection which regulate and discipline the international transfers of personal data. The activity of processing personal data for the purposes mentioned above is regulated in particular by Instruction no. 49 *"On the protection of personal health-related data".*

The above mentioned guidelines set forth that the retention period of the collected data will be for as long as necessary in order to address legal requirements in the context of measures against COVID-19.

Upon the termination of the epidemic surveillance, the data must be anonymized/pseudonymized as regards to further processing purposes which may be used for statistics, scientific purposes, etc.

3. Sharing of health data with law enforcement agencies

Pursuant to point 42 of Article 3 of Law 15/2016, "Epidemic Surveillance" is the systematic collection, recording, analysis, interpretation and dissemination of data and analysis on infectious diseases and other health issues related to them, on regular basis, to gain knowledge about the disease, its spread and to take actions to eliminate, eradicate, control and prevent it.

On the legitimate processing of personal data, the IDP has developed and published specific guidelines and good practices for the collection, processing, disclosure, security, etc., of health data in the context of measures against COVID-19.

The IDP has published, inter alia, Instruction No. 49 "*On the protection of health-related personal data*" and Instruction No. 47 "*On determining rules on safeguarding personal data processed by large processing entities*". The guidelines provide technical and organizational measures which should be taken by controllers prior to the processing of personal/health data.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Albania on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The IDP Albania has not faced any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

The Commissioner's guidelines anticipate the best practices in guaranteeing legitimacy of data processing during the situation "**work-from-home / return-to-work**".

The Office of the Commissioner has published the Guidelines for the processing of personal data according to the Protocols of Hygienic-Sanitary Measures COVID-19, which is organized in the form of Q&A, addressing various situations related to the processing of personal data which consist of:

i. Collection of health data for employees and visitors;
ii. Measures to be taken by the controller/employer in the framework of personal data protection;
iii. Criteria for determining the person responsible for data processing and his responsibilities;
iv. Information and manner of providing Information on data processing in the framework of measures taken against COVID-19;
v. Instructions for the dissemination or publication of data;
vi. Instructions for the retention period of health data of employees and visitors; and
vii. Instructions for the necessary technical and organizational measures to guarantee the security and confidentiality of personal data; etc.

Andorra - Andorran Data Protection Agency (Agència andorrana de protecció de dades) (APDA)

1. Contact tracing and location tracking

An app of contact tracing is being developed but it hasn't been adopted yet.

During the development of this digital contact tracing app the Andorran DPA issued a report about the project, assessing its functionalities and its respect to data protection rules and standards. This report was given both to the administration and to the early developers of the app.

Also, this Authority has an oversight role to all data protections issues that may arise in Andorra according to the Qualified Act 15/2003 of Data protection and accordingly, an eventual app on contact tracing will be subjected to the control and oversight of this Authority.

The Authority required from the early developers of the app a Privacy Impact Assessment, which was responded to. This proved that the developers were following the general instructions and principles entitled to all data processing such as the minimisation of the collection of personal data, the quality of the data, transparency, etc.

Here are some links provided to the general public about data principles that needed to apply to data processing in the context of the COVID and in general processing (in Catalan):

- https://www.apda.ad/sites/default/files/2020-03/COVID19.pdf
- https://www.apda.ad/sites/default/files/2019-06/Deure%20d%27informaci%C3%B3_0.pdf
- https://www.apda.ad/sites/default/files/2018-11/Gu%C3%ADa%20legal%20de%20creaci%C3%B3%20de%20apps..pdf
- https://www.apda.ad/sites/default/files/2019-06/el%20principi%20de%20proporcionalitat.pdf

However, this Authority hasn't been able to monitor the efficacy of the app as it hasn't been fully developed yet. That's why the Authority considers that the measures are

not taken yet as the Andorran Data Protection Agency hasn't issued a report about the final version of this digital measure.

2. Sharing of health data with health authorities and institutions

According to the Health Act of 2009, the Andorran Health authorities are authorised to collect, process and share health data during emergency states and pandemics and share those with the Government in order to prevent the spread and to activate mechanisms of control. The data included in these communications will be the name of the particulars and their health status. This competence shall be activated by an Ordinance issued by the government (as per in the Ordinance of March 13th 2020 https://www.bopa.ad/bopa/032021/Pagines/GD20200312_11_51_13.aspx).

According to the act, this data sharing will be allowed as long as there is a legal basis for it and that the communications respect the dispositions of the Qualified Act on Data Protection of 2003.

The data shared with public health authorities will be retained for research in public interest. This data retention will be held to the general standards of data protection. This means that the data will be preserved for the period of time necessary to fulfill the purpose of its collection. The anonymisation of that data has been recommended by this Agency to the Health Authority.

As the communication between those institutions is ruled by the Data Protection Act, the Andorran Data Protection Agency has the role to oversee those data sharing. During the emergency state, the Andorran DPA issued a series of guidelines aiming at health professionals and authorities about data protection. On those, the Authority focused on the need of having a legal basis to the data processing, the limitations of purpose as a data protection principle, the need to inform the particulars about the use of their data and the need to establish a procedure of privacy by design in all processing done (among others). Here is a link to the Guidelines published (in Catalan): https://www.apda.ad/sites/default/files/2020-04/tractaments%20dades%20autoritats%20publiques%20%281%29.pdf .

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in Andorra on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Andorra on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The Andorran DPA has not faced any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

The major privacy issues identified by the Authority in the handling of employee data in work-from-home were the need to ensure the confidentiality of the data that might be processed on this and the need to remind the employers about the privacy held by their employees on the data stored on their devices.

Also, this Authority focused on the legal obligation established in the Health and Security at Work Act that obliged employers to guarantee good health in the workplace. Also, in the Ordinances issued by the Government during the Emergency State, some instructions were made to employers on this subject.

To promote good practices in addressing or mitigating the privacy issues associated with the handling of employees' personal data in work-from-home/return-to-work situations identified above, this Authority published 3 documents related to these subjects (documents are in Catalan):

- An infographic about the assurances of security and confidentiality in work-from-home employees: https://www.apda.ad/sites/default/files/2020-03/teletreball.pdf
- Guidelines focused to the processing of data of employees directed to employers: https://www.apda.ad/sites/default/files/2020-03/COVID19.pdf
- Guidelines on collecting temperature both in the workplace as in other public areas: https://www.apda.ad/sites/default/files/2020-05/280520132326.pdf

Australia - The Office of the Australian Information Commissioner (OAIC)

1. Contact tracing and location tracking

Developer:

The Australian Government's Department of Health, with support from the Digital Transformation Agency, has developed the **COVIDSafe app** as a digital tool to assist the manual process employed by state and territory health authorities to identify and contact people exposed to the COVID-19 virus.

Voluntary or Mandatory?

The COVIDSafe app is a voluntary and consent-based application.

Technology of digital measure:

To use the COVIDSafe app, individuals must provide:

- a name (this can be a pseudonym);
- age range;
- mobile number; and
- post code.

Based on this information, the COVIDSafe app generates a user ID which is automatically encrypted and stored in the COVIDSafe app on the individuals' phone. All registration information, encrypted user IDs and contact data is stored in the National COVIDSafe Data Store. The COVIDSafe app uses Bluetooth technology to look for other devices that have the app installed. It takes note of a contact when it occurs, through a digital handshake. It securely logs the other user's encrypted reference code, the date, time, Bluetooth signal strength and proximity of the contact on the user's phone, and phone model. The COVIDSafe app does not record the name, phone number, age or postcode of other people, or any location information.

How information is stored, disclosed and used:

The COVIDSafe app encrypts and stores contacts on the phone for 21 days, and deletes contacts older than 21 days. This allows for the 14-day incubation period of COVID-19,

and the time taken to confirm a positive test result. If an individual has tested positive for COVID-19, a state or territory health official will ask the individual to consent to uploading their information from the COVIDSafe app to the National COVIDSafe Data Store. Contacts are reconciled with registration information within the National Data Store and made available to limited contact tracers within the relevant health authority.

Assessment of privacy risks:

Under the Australian Government Agencies Privacy Code, Australian Government agencies are required to complete a Privacy Impact Assessment (PIA) for high risk privacy projects. The Department of Health completed a PIA when developing the COVIDSafe app, and consulted with the OAIC. The OAIC's key recommendation was for legislation to be established to enshrine strict privacy safeguards to govern the collection, use and disclosure of COVID app data.

The Government published the PIA and accepted the recommendations: https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment#:~:text=The%20PIA%20identifies%20the%20impacts,a%20response%20to%20the%20recommendations

The Australian Government's PIA set out 19 recommendations to address privacy risks, including a recommendation that legislation be developed to enshrine strong privacy protections concerning COVID app data. The Australian Government accepted this recommendation. Prior to legislating privacy protections, the COVIDSafe app was supported by interim privacy protections outlined in a determination made under the *Biosecurity Act 2015*.

Measures to address privacy and security risks:

The Australian Government enshrined privacy and data security safeguards for the COVIDSafe app in legislation by making legislative changes to the *Privacy Act 1988* (Privacy Act).

The legislative amendments introduced several privacy protections, including:

- the incorporation of the purpose limitation principle (COVID app data is only to be used for contact tracing purposes);
- the introduction of new criminal offences, such as coercing or requiring someone to download or use the app, unauthorised collection, use or disclosure of COVID app data. (Criminal offences can be investigated by the

Australian Federal Police. The maximum penalty for breaches is five years imprisonment or a $63,000 fine);

- the expansion of the OAIC's regulatory oversight to state and territory health authorities, and stronger assessment powers over the COVIDSafe system;
- that once the Health Minister has determined that the COVIDSafe app is no longer needed to prevent or control the spread of the virus, all data in the National COVIDSafe Data Store will be deleted as soon as is reasonably practicable, and users will be informed;
- the application of the notifiable data breach scheme to include certain conduct by the National COVIDSafe Data Store administrator, and state and territory health authorities in relation to the handling of COVID app data; and
- the Privacy Commissioner's obligation to report publicly every six months on the performance of the Privacy Commissioner's functions and exercise of the Privacy Commissioner's powers under the new COVID app-related provisions of the Privacy Act.

Consultation with the OAIC:

The OAIC engaged closely with the Australian Government and was consulted on the PIA and draft legislation. The OAIC engaged with our international counterparts to gain insight into best practice responses to privacy issues.

Roles conferred to the OAIC:

The new law governing the handling of COVID app data provides for an expansion of the OAIC's regulatory oversight and enforcement powers. This includes the handling of COVID app data by state and territory health authorities, in addition to existing powers to regulate the Commonwealth in its handling of the National COVIDSafe Data Store.

The OAIC can proactively assess the COVIDSafe system to identify privacy risks and has expanded powers to compel information and documents. Individuals can make complaints to the OAIC about the handling of their personal information within the COVIDSafe system. Data breaches relating to the COVIDSafe system must be notified to the OAIC, whether they occurred at a federal or state level.

Under the amended legislation, the OAIC is the independent regulator of the COVIDSafe system, and is actively monitoring and regulating compliance with relevant provisions in the Privacy Act. The OAIC has powers to:

- conduct audits;
- investigate complaints;

- order compensation to be paid to individuals who suffer from an interference with their privacy;
- seek civil penalties against individuals and organisations which breach the law;
- refer matters to the police if we think a crime has been committed; and
- refer matters to state and territory privacy regulators if appropriate.

The OAIC has published a dedicated page online to provide specific guidance on good privacy practices in the context of the COVID-19 pandemic for individuals, Australian Government agencies and organisations covered by the Privacy Act.

Good practices promoted by the OAIC:

Under Australian legislation, Australian Government agencies are required to complete a Privacy Impact Assessment (PIA) for high risk privacy projects. For the COVIDSafe system, the Department of Health conducted a PIA and consulted with the OAIC.

The OAIC advocated for a legal framework to be established that would engender public trust and confidence in the use of the COVIDSafe app, and promoted privacy by design principles:

- purpose limitation principles;
- use and disclosure limitations, and transparency requirements;
- the consideration of proportionality and necessity requirements;
- data minimization principles;
- storage limitation; and
- data security.

Generally, the OAIC encourages entities to consider the following points:

- personal information should be used or disclosed on a 'need-to-know' basis;
- only the minimum amount of personal information reasonably necessary to prevent or manage COVID-19 should be collected, used or disclosed;
- consider taking steps now to notify staff how their personal information will be handled in responding to any potential or confirmed case of COVID-19 in the workplace; and
- entities should ensure reasonable steps are in place to keep personal information secure, including where employees are working remotely.

Further sources:

For more Australian Government information on the COVIDSafe app, see:

- https://www.covidsafe.gov.au/
- https://www.health.gov.au/resources/apps-and-tools/covidsafe-app.

The OAIC has released privacy guidance on COVID-19 and contact tracing:

- https://www.oaic.gov.au/updates/news-and-media/covid-19/.

2. Sharing of health data with health authorities and institutions

Under the new law, information that has been collected or generated through the COVIDSafe system can only be collected, used or disclosed by:

- state or territory health officials who are contact tracing individuals possibly exposed to COVID-19;
- the administrators of the COVIDSafe app and the National COVIDSafe Data Store, to enable the app, the Data Store and contact tracing to work properly and to ensure the integrity of the app and Data Store; or
- the OAIC and police enforcing these privacy protections.

Information that has been collected or generated through the COVIDSafe app cannot be accessed by police, or used in court proceedings, except where the suspected offence is a breach of Part VIIIA of the Privacy Act.

COVIDSafe app information about an individual that is collected by a state or territory health department is protected by the Privacy Act.

COVID app data will not be retained for research in the public interest.

3. Sharing of health data with law enforcement agencies

Under the amended legislation, COVID app data can only be used for contact tracing purposes by state or territory health officials who are contact tracing individuals possibly exposed to COVID-19. It cannot be used for law enforcement purpose, except for purposes that relate to the enforcement of the privacy protections enshrined in the law.

4. Sharing of health data with charitable or other similar organisations

Under the amended legislation, COVID app data can only be used for contact tracing purposes. As such, there is no requirement, arrangement or plan for sharing COVID app data with charitable or other similar organisations.

5. Handling of employee data in work-from-home / return-to-work situations

Information in this section concerns the handling of employees' personal information, generally, during the COVID-19 pandemic. It does not concern the COVIDSafe app or the handling of COVID app data, which has been addressed separately in the sections above.

On the matter of personal information, generally, the OAIC appreciates the unprecedented challenges that Australian Government agencies and private sector organizations are facing to address the spread of COVID-19. The Privacy Act will not stop critical information sharing for public health purposes. Agencies and private sector employees (including private health service providers) have important obligations to maintain a safe workplace for staff and visitors and handle personal information appropriately. For private sector employees, the employee records exemption within the Privacy Act will apply in many instances to permit the handling of employee health information.[5]

At present, the OAIC has have identified the following privacy issues in relation to the (1) handling of employee data during work from home circumstances; and (2) the handling of employee data in return to work circumstances:

- the collection, use and disclosure of employees' personal information, in particular, the collection of sensitive information;
- whether the collection of such information is reasonably necessary, or directly related to, one or more of an agency or businesses' functions or activities, such as to prevent or manage COVID-19 in the workplace; and
- the security and confidentiality of employees' personal information.

The OAIC has developed advice and guidance on privacy in the context of the COVID-19 outbreak for individuals, Australian Government agencies and organisations covered by the Privacy Act:

[5] For example, a record about a private sector employee's sick leave falls within this exemption where it is used or disclosed for a purpose directly related to a current or former employment relationship between the employer and individual.

- Privacy guidance for agencies and private sector employers to help keep workplaces safe and handle personal information appropriately, including answers to frequently asked questions;
- Detailed advice to help regulated entities assess the privacy risks involved in changed working environments and remote working arrangements; and
- A step-by-step tool to help guide organisations and agencies through the Privacy Impact Assessment process.

I. Handling of employee data during work-from-home circumstances

The Privacy Act does not prevent employees from working remotely as a response to COVID-19. However, the Australian Privacy Principles will continue to apply. Australian Government Agencies and employers will need to consider security measures for employees working remotely, as those that apply in normal circumstances.

The OAIC advises that regulated entities should consider whether any changes to working arrangements will impact the handling of personal information, assess any potential privacy risks, and put in place appropriate mitigation strategies as part of Business Continuity Planning. A PIA is a useful tool for evaluating and mitigating risks to personal information.

Through the provision of general guidance for businesses, the OAIC advises that Australian Government agencies and businesses should:

- use and disclose personal information only on a 'need-to-know' basis;
- collect, use and disclose only the minimum amount of personal information reasonably necessary to prevent or manage COVID-19;
- consider taking steps to notify staff of how their personal information will be handled in responding to any potential or confirmed cases of COVID-19 in the workplace; and
- ensure reasonable steps are in place to keep personal information secure, including where employees are working remotely.

II. Handling of employee data in return-to-work situations.

Through the provision of our guidance for businesses, the OAIC advises that as it relates to the handling of employees' personal information, generally, businesses should:

- only collect personal information for contact tracing purposes;
- notify individuals before personal information is collected;
- securely store information once they have collected it;

- provide information to relevant health authorities who undertake contact tracing activities, when requested to do so; and
- destroy personal information once it is no longer reasonably necessary for the purposes of contact tracing.

The OAIC has received one complaint concerning the handling of employee data in a work-from-home / return-to-work situation. This is an open file and the OAIC will attempt to resolve the matter through its early resolution processes.

Australia (Victoria) - Office of the Victorian Information Commissioner (OVIC)

1. Contact tracing and location tracking

The federated nature of Australia means that some responses to COVID-19 were coordinated by the federal government, and some by the state and territory governments.

In April 2020, the federal government launched the voluntary 'COVIDSafe' app for Australian jurisdictions. The Australian Government's app aims to **facilitate state and territory health officials across Australia** to conduct contact tracing to stop the spread of COVID-19. The Australian Government stores the contact tracing data collected via the app, with access limited to relevant state or territory health officials to conduct contact tracing in their jurisdictions.

The app uses bluetooth to look for other devices that have the app installed, noting when contact occurs. It securely logs the other user's encrypted reference code and the date, time, bluetooth signal strength and proximity of the contact on the user's phone, and notes the phone model. This information is then securely encrypted and stored on the phone for a period of 21 days.[6]

From a Victorian perspective, some businesses, workplaces and premises must request that each person who attends the premise for more than 15 minutes provide their first name and phone number, to support contact-tracing. Information to support businesses and workplaces understand their record-keeping obligations for contract tracing purposes is available on the Victorian Department of Health and Human Service's (**DHHS**) website.[7]

DHHS' website is updated daily to ensure the public and service providers have access to updated information regarding the management of COVID-19.

The Office of the Australian Information Commissioner (**OAIC**), the federal privacy regulator in Australia, established a National COVID-19 Privacy Team, comprising

[6] More information about the design of the Australian Government's COVIDSafe app is available here: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

[7] See, https://www.dhhs.vic.gov.au/record-keeping-contact-tracing-covid-19.

senior representatives from privacy authorities across Australia. This was the forum for much of the consultation with state and territory privacy authorities, to provide updates on the development of the COVIDSafe app, as well as relevant guidance regarding contract tracing measures, to ensure consistency in messaging and understanding across jurisdictions.

The relevant health authority in Victoria, DHHS, consulted with OVIC regarding DHHS' use of the data collected via the COVIDSafe app for the purposes of contact tracing.

Addressing privacy risks of the App:

The Australian Government commissioned a privacy impact assessment (**PIA**)[8] when developing the COVIDSafe app and responded[9] directly to the 19 recommendations made, including:

- seeking consent of app users at multiple points – ensuring consent at the initial registration stage and the upload stage;
- contractual or other arrangements with state and territory public health authorities, to ensure appropriate security arrangements and that the data is only used for authorised purposes; and
- ensuring that the Notifiable Data Breaches Scheme,[10] currently in place for Australian government agencies, will apply in relation to information collected by the app.

As a further protection, the *Privacy Amendment (Public Health Contact Information) Act 2020* was passed, to codify protections for data collected via the app, including:

- ensuring that the OAIC (federal privacy regulator) in Australia has oversight of the COVIDSafe data;
- the deletion of COVIDSafe data at the end of the COVID-19 pandemic, and users to be notified accordingly; and
- requirements for the Minister for Health to report on the operation and effectiveness of the COVIDSafe app and the National COVIDSafe Data Store every 6 months.

OVIC was consulted on the implementation of the COVIDSafe app via the National COVID-19 Privacy Team.

---

[8] Available here: https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment.
[9] Available here: https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment-agency-response.
[10] See https://www.oaic.gov.au/privacy/notifiable-data-breaches/.

DHHS is required to comply with federal privacy law in relation to its handling of COVIDSafe app data. In Victoria, the Health Complaints Commissioner (**HCC**) administers the *Health Records Act 2001*, that relates to the handling of health information of an individual. As such, the HCC has jurisdiction over non-COVIDSafe app data used in contact tracing (i.e. any other info gathered by DHHS for contact tracing, as it falls within the definition of health information).[11]

OVIC administers the Victorian Protective Data Security Framework (**VPDSF**)[12] that will apply to DHHS' handling of the data collected via the COVIDSafe app.

OVIC has published guidance on *Privacy and coronavirus*[13] outlining the obligations of Victorian Public Sector (VPS) organisations when collecting, using and disclosing personal information to manage the spread of COVID-19 in Victoria. The guidance also outlines the security measures that should be applied to data that is handled by VPS organisations in responding to COVID-19.

DHHS consulted with OVIC on the PIA commissioned regarding the use of the data collected via the COVIDSafe app to conduct contact tracing in Victoria.

OVIC encouraged DHHS to ensure transparent and consistent messaging around the use of the COVIDSafe data, to gain the public trust necessary for the app's success. In terms of DHHS' obligations under the VPDSF, OVIC suggested the following best practice measures to DHHS:

- deletion of data once no longer useful for the purposes of contact tracing (taking into account overarching record-keeping obligations);
- that any research conducted using the data should be in a secure environment, with a range of protections beyond just technical measures such as encryption in place – like restrictions on physical access;
- voluntarily advising OVIC of any privacy breaches that may occur in relation to the COVIDSafe data.

[11] More information about the role and jurisdiction of the HCC is available here: https://hcc.vic.gov.au/about/our-organisation.
[12] Available here: https://ovic.vic.gov.au/data-protection/framework-vpdsf/.
[13] Available here: https://ovic.vic.gov.au/resource/privacy-and-covid-19/.

2. Sharing of health data with health authorities and institutions

***As regulation of personal information and health information is spilt over two authorities in Victoria, OVIC and the HCC respectively, OVIC is not the best placed authority to provide a response to this question. ***

3. Sharing of health data with law enforcement agencies

***As regulation of personal information and health information is spilt over two authorities in Victoria, OVIC and the HCC respectively, OVIC is not the best placed authority to provide a response to this question. ***

4. Sharing of health data with charitable or other similar organisations

***As regulation of personal information and health information is spilt over two authorities in Victoria, OVIC and the HCC respectively, OVIC is not the best placed authority to provide a response to this question. ***

5. Handling of employee data in work-from-home / return-to-work situations

At the time of writing, OVIC was not aware of any privacy breaches in relation to employee data, as a result of work-from-home arrangements.

At the commencement of remote working arrangements, OVIC published guidance to assist VPS organisations adhere to privacy obligations while working from home. The guidance *How to respect privacy and protect public sector information when working remotely – tips for VPS employees*[14] provides very practical, introductory information for VPS organisations and employees regarding privacy best practice while working from home. Tips include:

- avoiding working in public places and set up a private workspace where possible;
- using a secured WiFi network or ethernet; and
- securing devices and documents at the end of the day.

OVIC has also published guidance on *Collaboration tools and privacy*,[15] providing VPS organisations with helpful tips on using videoconferencing and instant messaging programs to facilitate working from home arrangements. Some privacy best practice measures include:

[14] Available here: https://ovic.vic.gov.au/privacy/for-agencies/guidance-and-resources/short-guides/.
[15] Available here: https://ovic.vic.gov.au/wp-content/uploads/2020/06/Collaboration-tools-and-privacy.pdf.

- conducting privacy impact and security risk assessments (on chosen collaboration tools) and reviewing these periodically;
- developing internal terms of use policies; and
- conveying clear expectations for use to employees.

OVIC also has general guidance on workplace privacy,[16] that includes information regarding privacy best practice when working from home.

[16] Available here: https://ovic.vic.gov.au/wp-content/uploads/2020/04/Workplace-Privacy-Information-Sheet.pdf.

Belgium - Belgian Data Protection Authority

Autorité de protection des données
Gegevensbeschermingsautoriteit

1. Contact tracing and location tracking

Belgium has adopted both manual and digital contact tracing and location tracking measures:

Manual measures:

- contact tracing regional call centers;
- A manual registration of clients in bars and restaurants: obligation for bars and restaurants to collect the name and contact data (e-mail address and phone number) of clients - 1 client per table - in order to be able to contact them in case of a Covid-19 contamination. The personal data are stored 14 days. Legal basis being: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2020063002&table_name=loi (cf. Article 5) and http://www.ejustice.just.fgov.be/eli/arrete/2020/07/28/2020031151/moniteur (cf. Article 3)
- The "Public Health Passenger Locator Form": Belgian citizens traveling abroad are asked to fill out the Public Health Passenger Locator Form.
- Data collected: name, sex, date of birth, national number ('Rijksregisternummer'), contact data (telephone number, e-mail address) and in some cases, health data (diagnosis, test results, symptoms, etc.)
- The manual measures are mandatory (registration of individuals who tested positive for Covid-19 and individuals presumed 'positive' or for whom a COVID-19 test is prescribed by a health professional; and the contacts of the individuals mentioned before; registration in bars and restaurants, the Public Health Passenger Locator Form).

Digital measures:

- Location tracking based on anonymous telecom data; and
- The Coronalert application, which will be operational later in September 2020, by use of BLE (Bluetooth) technology. Legal basis being: http://www.ejustice.just.fgov.be/eli/arrete/2020/06/26/2020041950/moniteur

- An opinion from our authority on the upcoming application has recently been published: https://www.autoriteprotectiondonnees.be/citoyen/chercher?q=&search_category%5B%5D=taxonomy%3Apublications&search_type%5B%5D=advice&s=recent&l=25.
- The digital measures are implemented by the local authorities in collaboration with Sciensano, a public institution with legal personality which performs public health assignments. The contact tracing application was developed by a private company (Devside).
- How the digital measures work: An opinion from our authority on the upcoming application has recently been published: https://www.autoriteprotectiondonnees.be/citoyen/chercher?q=&search_category%5B%5D=taxonomy%3Apublications&search_type%5B%5D=advice&s=recent&l=25
- Data collected: name, sex, date of birth, national number ('Rijksregisternummer'), contact data (telephone number, e-mailaddress) and in some cases, health data (diagnosis, test results, symptoms, etc.).
- The digital measures (esp. the contact tracing application) are voluntary.

As far as the digital measures are concerned, the Belgian DPA was consulted for analysis of the legal basis and the Data Protection Impact Assessment (DPIA), in accordance to Article 35 GDPR. It was also consulted for the manual measures.
The Belgian DPA published a series of advice on balance between the protection of privacy and the protection of public health:
https://www.autoriteprotectiondonnees.be/citoyen/themes/covid-19

2. Sharing of health data with health authorities and institutions

There is a legal requirement for hospitals and labs to share health data with Sciensano and local/regional contact tracing centers. The kinds of health data that will be shared are identification and contact data, tests results, prescriptions, CT-scan examination results and presumptive diagnoses, data relating to the infected or seriously suspected of being infected, as well as hospitalized patients with a coronavirus diagnosis if has been confirmed in hospitals.

The authority's advice to government is published on
https://www.autoriteprotectiondonnees.be/citoyen/themes/covid-19.

The limitation on the retention of data is 60 days maximum (for central database). Pseudonymisation measures have been adopted.

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in Belgium on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Belgium on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The Règlement général sur la protection des données (RGPD) and other usual laws apply, but more specific advice is provided on our website:
https://www.autoriteprotectiondonnees.be/citoyen/themes/covid-19/covid-19-sur-le-lieu-de-travail

Bulgaria - Bulgarian Commission for Personal Data Protection (CPDP)

1. Contact tracing and location tracking

Some amendments are made to the Law on Electronic Communications, namely an obligation for the mobile operators, internet providers and members of the electronic communications networks and services to collect location data of the persons deviating from (refusing or not executing) isolation/confinement. Right to access to this data is granted to the Ministry of Interior and its territorial divisions after a decision of the competent district court.

The National Operational Headquarters for the fight against COVID-19 unveiled a mobile app "Virusafe"(developed by Scalefocus) aimed at assisting the competent authorities in organizing and controlling the anti-epidemic measures imposed in the country. The controller of the personal data processed through the app is the Ministry of Health. The app is entirely voluntary for the citizens and data processing, including those for the health and location of individuals is made solely on the basis of consent.

The application has features, specifically built to support the fight against COVID-19. The current version of ViruSafe has the following:

- Daily symptoms and health status tracker;
- Location tracker, enabled voluntarily by the user, to create a heatmap with potentially infected people;
- Notifications, which inform users on hot news, related to COVID-19; and
- Information and best practices, connected to the pandemic.

In order to enable the full range of features of the application, users need to enter personal data, such as personal ID, age, any chronical diseases they may have and allow the app to use their location. This in turn will give Ministry of Health and local authorities all necessary information, in case further actions are needed.

All personal data is accessible only by Ministry of Health and authorized governmental institutions.

The Commission for Personal Data Protection has been consulted on the Virusafe Privacy Policy and the comments and recommendations were taken into account before the publication of the Policy.

The tracking app was developed, taking into account all the requirements of the EU and national data protection legislation including the DPIA, privacy by design measures using specific digital tools, which are subject to review by the controller and the DPA. The location tracking is enabled on voluntary basis with user consent. Personal data, including health data, are sent to the concerned authorities only after consent from the individual. There is a short version of the application, which allows the user to receive relevant information about the spreading of the Covid-19 without providing personal data to the app and the authorities. The data will be collected and further processed for a limited period (until the existence of epidemic/pandemic situation).

The penalties, which could be imposed if data protection violation is established by CPDP, are set in the relevant EU and national legislation.
The Commission for Personal Data Protection has been consulted on the tracking app and has regulatory and consultative competences in accordance with the EU and national personal data protection legislation.

The Commission for Personal Data Protection promotes the application of the EU and national data protection legislation and all the rules and requirements stemming from them with regard to the use of the contact tracing or location tracking measure. Awareness raising information and documents have been published on the official site (www.cpdp.bg).

2. Sharing of health data with health authorities and institutions

Users need to enter information about the current symptoms of any chronical diseases they may have and allow the tracking app to use their location. The information will be submitted to the Ministry of Health, the regional health inspectorate, the individual's general practitioner and the relevant laboratory.

In this regard, the Commission for Personal Data Protection has supervisory and advisory competences and cooperates effectively with the relevant authorities.

The rules for sharing data with health authorities are established in the specific legal acts taking into account the EU and national data protection legislation. The collected personal data could be additionally used for statistical, scientific or historical research

purposes following the requirements of Art. 89 of the GDPR (pseudonymisation or anonymization).

3. Sharing of health data with law enforcement agencies

Personal data will be shared with the Ministry of Interior and the Fire department for the purpose of protecting the public order and national security. The information is needed in order to observe the people with Covid-19, who are quarantined.

The Commission has advisory and supervisory role with regard to the data sharing arrangement. The rules for sharing data with law enforcement agencies are established taking into account the EU and national data protection legislation.

The main principle is of data minimisation and limitations of purposes. The police authorities are provided with the strict minimum of information by the Ministry of Health in order only to follow up the quarantine measures.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Bulgaria on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic. Personal health data will be shared with the municipalities (specific units), which are responsible for offering support and assistance to the citizens in need.

5. Handling of employee data in work-from-home / return-to-work situations

Currently, no complaints or data breaches have been submitted with regard to employee data in work-from-home/return-to-work situations.

So far, no privacy issues have been identified with regard to employee data in the context of work-from-home. As it comes to return-to-work situations, the constant position of the CPDP is that the medical information (including COVID-19 results) is not part of the information suitable for processing from the employers – this data should be processed only by competent medical authorities with regard to professional secrecy. Employers can process medical data only afterwards – while handling the documents for medical relief for example, also with regard to professional secrecy. All other necessary measures (as quarantine for the contact persons, disinfection of the working places etc.) are entirely of the responsibility of the national and regional health and sanitarian bodies.

Nevertheless, the CPDP issued several observations on the processing of medical data in working environment.

Currently, no complaints or data breaches have been submitted with regard to employee data in work-from-home/return-to-work situations.

Burkina Faso - Commission de l'Informatique et des Libertés (CIL)

1. Contact tracing and location tracking

Mobile Applications

- Corona-Detect is an application open to the general public that allows each user to self-diagnose in order to obtain rapid follow-up and support when needed;
- Corona-Contact is an application dedicated to people who have had contact with a confirmed or probable case of Covid-19. It will inform on a daily basis the evolution of symptoms during the follow-up period;
- Corona-Corus is an application that allows medical teams at each health level to analyse alerts that users have sent through Corona-Detect;
- "l le Mondjossi," is a mobile application linking geolocation and supported by live chat.
- For all of these applications, the installation is voluntary for the individuals involved and the data collected relate to the identification and geolocation of the user. Details of these applications can be found here: https://www.surveillance-sante.bf/.

Role of the Commission

- The Commission as the data protection authority has not been involved in the development of these solutions. But playing its full role through meetings with the health authorities, it drew their attention to the consideration of the protection of personal data.
- Since the beginning of the pandemic, the CIL through TV spots, TVfilms, interviews and video conference communications, communicates to the health authorities with a view to taking into account the principle of confidentiality which is a cardinal principle in the protection of personal data.

2. Sharing of health data with health authorities and institutions

There are requirements/arrangements in Burkina Faso on sharing of health data with health authorities and institutions for fighting COVID-19.

Article 11 of the 20 April 2004 Personal Data Protection Act 010-2004 provides that data treatments for the purpose of individual therapeutic or medical follow-up of patients are not subject to the provisions of the latter. The fight against the pandemic falls within the framework of this derogation. However, the Commission constantly reminds those responsible for sharing that, notwithstanding this derogation, compliance with the principles of data protection remains. In addition, section 21, paragraph 3 of the aforementioned law, authorizes sharing without the consent of the person concerned, in the event that treatment is necessary to safeguard the life of the person concerned or that of a third party.

The Commission, as a national data protection authority, provides advice and control to health authorities in the data sharing process.

In the data-sharing process, the Commission promotes the following best practices:

- The requirement for prior formalities for the processing of personal data through the declaration of treatment to the supervisory authority;
- Respecting the principles of security and confidentiality;
- Respecting the purpose of the treatment; and
- Respect for people's data processing rights.

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in Burkina Faso on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

A protocol has been developed in Burkina Faso for sharing the data of those in need between the state and the agencies involved in the social protection of those in need. The protocol sets out the conditions for data sharing of destitute people for their care. In accordance with the law, this protocol gives the Commission the power to monitor respect for the rights of individuals in the process of sharing data between actors.

The best practices promoted by the Commission in this data sharing protocol are:

- The requirement to complete the formalities;
- Respect for proportionality in data collection;
- The purpose of the treatment is the result;
- Confidentiality and security measures; and
- Respect for people's rights.

5. Handling of employee data in work-from-home / return-to-work situations

The main privacy issues identified in relation to handling of employee data in work-from-home/return-to-work situations can be summed up as follows:

- Risk of exposure to his private life and that of his family;
- Network security vulnerabilities; and
- Reliability of telecommuting applications.

The Commission shares with employees the following best practices:

- Ensure a secure internet connection;
- Promote the use of equipment supplied and controlled by the company;
- If you use a personal computer, make sure it is secure enough; and
- If you use a personal phone, protect your data and limit access.

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

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

1. Contact tracing and location tracking

The COVID Alert App

In July 2020, the Canadian federal Department of Health funded and made available a national COVID-19 exposure notification app, COVID Alert. It is meant to be interoperable across provinces, though each Canadian province or territory will have the option to adopt the app for its jurisdiction.

At present (Oct. 16, 2020), 4.3 million individuals have downloaded the application. Eight of ten provinces in Canada have now either confirmed usage or their immediate intention to adopt the federal application. The remaining two provinces and territories are actively considering its use.

COVID Alert, was adopted and adapted from source code (COVID Shield) made publicly available in May. Both apps use the Google-Apple Exposure Notification (GAEN) API issued in April.

Use of COVID Alert is voluntary for individuals. Once the app is fully functioning in a province or territory, users who test positive for COVID-19 will receive a one-time key from their provincial health authority that they can enter into the app. When the key is entered, COVID Alert will notify other users who may have come in close contact with that person for at least 15 minutes in the past 14 days, so they can contact their local public health authority for guidance.

While provincial health authorities collect and retain personal health information, the federal app relies on de-identified data, including random numbers that are not associated with individuals. At the critical point, when an individual is diagnosed with COVID-19 and provincial health authorities provide a one-time code for the individual to enter into the application, care is taken to ensure their identity is well protected. For instance, the matching of random numbers following an exposure only takes place on users' phones and no personal data will leave a user's phone.

The app is intended to complement existing measures to reduce the spread of the virus, including manual contact tracing.

Health Canada published its privacy assessment of the app which provides full details of its functioning: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy/assessment.html.

The OPC has also published its review of the app: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/

Involvement of the OPC regarding the development of the app

The OPC had several communications with government officials over the course of several weeks, reviewed Health Canada's privacy assessment[17] and issued our final review of the COVID Alert application on July 30, 2020.[18] While ideally the OPC would have preferred earlier consultation, the OPC was ultimately satisfied with the nature of the consultation that occurred.

Throughout the process, Health Canada and other federal partners communicated with the OPC on program details as they evolved, albeit over a compressed period. At the same time, several provincial data commissioners were engaging with health authorities in their jurisdiction.

The government was open to advice from the OPC and accepted several of our recommendations during the review process.

The OPC was generally pleased with the design of the federal government's exposure notification application.

With a view to achieving both greater flexibility and ensuring respect for privacy as a fundamental right, in April 2020 the OPC released a Framework to assess privacy-impactful initiatives in response to the pandemic ("the Framework")[19], which was followed shortly after by the issuance of a joint statement with provincial and territorial privacy commissioners on privacy principles that should be respected in the

[17] Health Canada, *COVID Alert: Exposure notification application privacy assessment* (August 2020) - https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy/assessment.html

[18] Office of the Privacy Commissioner of Canada, *Privacy review of the COVID Alert exposure notification application* (July 2020) - https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/

[19] OPC, *A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19* (April 2020) - https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/

design and during the use of any contact tracing or similar application ("the joint statement")[20]. Both of these documents were meant to offer clear guidance on how to incorporate privacy into the design of government programs to address the pandemic.

Our review concluded to our satisfaction that the Government had designed the app in line with the principles in both the Framework and joint statement. For example, strong measures ensure that the identity of users is protected and not disclosed to the Government of Canada. While experts generally agree that there is no such thing as zero risk of the re-identification of de-identified data, here, in light of the security measures and other safeguards adopted, the OPC determined that the risk of re-identification was very low.

The OPC concluded that the COVID Alert application had strong safeguards in place. In discussing the issue of destruction of data with Health Canada, the OPC was satisfied that significant steps had been taken to limit retention as much as possible, to delete data at regular intervals, and to shut down the application within 30 days after the declaration of the pandemic being over. Also important is that individuals can delete the application at any time.

There are oversight mechanisms in place that should help to verify the effectiveness of the application, among other factors. For example, the OPC offered to play an oversight role by conducting an audit one month after the launch of the app, and at a regular defined period thereafter. Health Canada has confirmed that it will conduct a joint audit with the OPC, to begin in the fourth quarter of 2020. The audit will include an assessment of respect for the principles in the joint statement of Canada's privacy commissioners, including an ongoing analysis of the application's effectiveness under the necessity and proportionality principle. If the OPC identifies problems during the course of the audit, the OPC will request that the government decommission the application.

Additionally, the government formed an External Advisory Council to provide advice and guidance so that "the application meets the highest standards in public health outcomes, technology and privacy". Members come from disciplines including health, privacy, data governance and science. Health Canada has committed to providing the OPC with regular reports on their work.

[20] OPC, *Supporting public health, building public trust: Privacy principles for contact tracing and similar* apps (May 2020) https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/

2. Sharing of health data with health authorities and institutions

The Memoranda of Understanding and contact tracing app

Specific to the case of Canada's COVID Alert app, there is a Memoranda of Understanding between the Canadian Federal Government and the Province of Ontario (the only province to have adopted the app at the time of writing).

The federal-provincial COVID Alert MOU includes rigorous privacy clauses, including that the Government of Canada will be using a "privacy-first approach", that the app does not collect or use location data and that the information transmitted by the app is designed to protect the user's identity or location.

The Government of Canada also commits in the agreement not to use the data it collects to identify or attempt to identify users unless for security purposes or when required by law, and to ensure the same of its service providers. The MOU includes requirements for Ontario to protect the one-time codes, to limit their retention and to delete them once they have been obtained by app users.

Additionally, the MOU requires Ontario to have security measures in place to address the potential vulnerabilities around the process by which users are given their one time code following a positive COVID-19 result. Finally, the MOU states that the app will be decommissioned within 30 days after the Chief Public Health Officer of Canada declares the pandemic over and that all data will be deleted from Canada's server, except for those related to active security incident investigations, within this period.
Moreover, there are a variety of laws which allow for orders to be made, which could entail special temporary measures to be taken in certain circumstances, such as a public welfare emergency. Federally, this would include the *Emergencies Act*, the *Quarantine Act*, and the *Department of Health Act*. There are a variety of provincial laws which would allow for similar measures to be taken to deal with emergencies.
Federal orders and regulations related to the pandemic are available on the following Government of Canada website:
https://www.justice.gc.ca/eng/csj-sjc/covid.html#wb-auto-4.

Involvement of the OPC Canada

While there is a policy requirement to inform the OPC of any planned initiatives that may have an impact on the privacy of Canadians, the OPC is not notified systematically. Currently both the conduct and the OPC's review of PIAs and the entering into of information sharing agreements and OPC's associated review remain at the level of policy requirements, rather than legal requirements.

The OPC generally receives information sharing agreements with associated PIAs, and provides advice on how the agreements may be improved to better protect privacy as part of the review of the PIA and associated documents.

Given that health related matters largely fall under provincial jurisdiction in Canada, the OPC does not have specific guidance in this regard. In relation to sharing personal information more generally, the Treasury Board of Canada Secretariat, which has a role for providing formal policy direction under the Privacy Act, has released *Guidance on Preparing Information Sharing Agreements Involving Personal Information.*[21]

OPC expects that institutions engaging in information sharing would assess risks via a privacy impact assessment (PIA). The OPC has published a guide for conducting PIAs which provides an overview of the process and steps to follow.[22]

The OPC has issued recommendations for reforming Canada's federal *Privacy Act* (which governs federal government departments' collection, use and disclosure of personal information). Part of our recommendations has included that written information sharing agreements be required by law and that they should be at minimum: define the specific elements of personal information to be shared; define the specific purposes for the sharing; and, limit secondary uses and onward transfer. Further, the OPC recommended that all new or amended agreements should be submitted to the OPC for review, and that existing agreements should be reviewable upon request. Finally, departments should be required to be transparent about the existence of these agreements.

3. Sharing of health data with law enforcement agencies

There are specific personal health information laws which fall under the jurisdiction of provinces. Information sharing specifically between provincial health authorities and local police forces therefore falls largely within provincial jurisdiction in Canada.

Federally, under PIPEDA, Canada's private sector privacy law, there are a variety of provisions under section 7(3) which would allow for the disclosure of personal information without knowledge or consent to law enforcement, such as if the disclosure is-

---

[21] Treasury Board Secretariat, *Guidance on Preparing Information Sharing Agreements Involving Personal Information* (July 2010) - https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html#a664Protectionof

[22] *Expectations: OPC's Guide to the Privacy Impact Assessment Process* - https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/

(c) *required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;*

(c.1) *made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that*

> ***(i)*** *it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,*
>
> ***(ii)*** *the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,*
>
> ***(iii)*** *the disclosure is requested for the purpose of administering any law of Canada or a province, or*
>
> ***(iv)*** *the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual;*

(d) *made on the initiative of the organization to a government institution or a part of a government institution and the organization*

> *(i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or*
>
> *(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;*

Under the federal *Privacy Act*, which governs federal government departments' collection, use and disclosure of personal information, section 8(2) contains a number of provisions that could potentially allow for personal information to be disclosed to law enforcement without consent:

> *(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;*
>
> *(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;*
>
> *(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;*
>
> *(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;*

The involvement of the OPC regarding these data sharing arrangements is similar to the above.

4. Sharing of health data with charitable or other similar organisations

There are **no** provisions specific to sharing health data with charitable or similar organizations offering support or assistance to those in need during COVID-19. That said, PIPEDA contains a provision which allows for disclosure of personal information without knowledge or consent if the disclosure is:

7(3)(f) *for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed.*

The *Privacy Act* contains the following provisions of potential relevance, which authorize the federal government to disclose personal information without consent:

- **8(2)(j)** to any person or body for research or statistical purposes if the head of the government institution
  (i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and
  (ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;
- **8(2)(m)** for any purpose where, in the opinion of the head of the institution,
  (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or
  (ii) disclosure would clearly benefit the individual to whom the information relates.

5. Handling of employee data in work-from-home / return-to-work situations

To date, no complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations have been received by the OPC Canada.

Through advisory work conducted by its Government and Business Advisory Directorates, the OPC has reviewed and offered recommendations on a number of programs or activities relating to employee personal data.

In relation to our review of various tools to track/report diagnosis information or the use of special leave codes (for employee absences related to COVID-19), the OPC has stressed:

- When reporting on employees' work and/or medical status, even in aggregate format, it is important to remember that there is always a significant risk of re-identification (and recommended taking administrative, technical, and physical means to protect the personal information collected).
- Ensure that personal information collected for these initiatives is disposed of as soon as it is no longer needed, except where retention is required to satisfy legal obligations.

On temperature screening of employees, the OPC has highlighted all of the principles in our Framework.[23] In particular, the OPC has stressed the need for such measures to be necessary and proportionate (meaning it should be evidence-based, tailored to the specific objective, and likely to be effective).

On the use of an electronic visitor logging and COVID-19 symptom monitoring system for employees, contractors, and visitors, the OPC has advised that:

- When a public sector institution stores sensitive personal information with a third party, there can be an elevated risk of impact in the event of a privacy breach. Consider ensuring that the contract includes strong privacy protection provisions.
- Reminder of the importance of being transparent with individuals about the potential disclosure of their personal information.
- Institutions should consider regular reviews of all COVID-19-related initiatives to determine whether they are still necessary, and have in place a plan to cease personal information collection when it no longer serves a business need.

The OPC has continued to engage with Parliamentarians, the business sector and the general public on how to maintain privacy protections while adapting to health measures and remote working. The OPC Blog had a feature "Videoconferencing – Maintain your physical distance, but keep your personal information close" (https://www.priv.gc.ca/en/blog/20200501/).

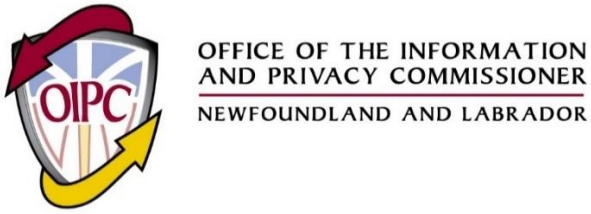
[23] https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid

The Office of the Privacy Commissioner of Canada, along with data protection and privacy authorities from around the world, also published an open letter[24]) to video teleconferencing companies reminding them of their obligations to comply with the law and handle people's personal information responsibly.

The letter is intended for all companies that offer video conferencing services, and has also been sent directly to Microsoft, Cisco, Zoom, House Party and Google. It provides video teleconferencing companies with principles to help them identify and address some of these risks and better protect the personal information of users.

[24] OPC, *Joint statement on global privacy expectations of Video Teleconferencing companies* (July 2020) - https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/let_vc_200721/

Canada (Newfoundland and Labrador) - Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC NL)



1. Contact tracing and location tracking

In Newfoundland and Labrador, there are four Regional Health Authorities (RHAs) that have responsibility for performing contact tracing. Contact tracing usually follows these steps:

- A person identified as possibly having a communicable disease, sometimes referred to as the index case, is interviewed to learn about their movements and with whom they have been in close contact during the time they could have been infected or infected others.
- Depending on the disease, family members, friends, work colleagues, health care providers, and anyone else who may have knowledge of the case's contacts may also be interviewed.
- When contacts are identified, Public Health Nurses contact them to offer counseling, screening, and if required, testing or treatment.

In addition to the manual process above, COVID Alert is also available for download through the Apple or Google Play app stores. This app was developed by the Government of Canada and its use is voluntary.

OIPC NL was engaged by the Department of Health and Community Services and the Newfoundland and Labrador Centre for Health Information in the early stages of development of a provincial app. These consultations included the private company developing the app, Verafin. Once the decision was made to leverage the COVID Alert app, the Office was kept informed through the Privacy Commissioner of Canada's Office. While the province did consult the OIPC NL again prior to launching the provincial iteration of the COVID Alert app, it could not really be considered early engagement.

The OIPC NL was brought into the consultation process on the national COVID Alert app by the Privacy Commissioner of Canada. Once the provincial government decided to leverage the COVID Alert app, OIPC NL conducted a review of provincial aspects. This included the messaging the individuals would receive if identified as a close

contact by the app, as well as the provincial usage of a federal portal that issues the one-time keys. While OIPC NL was not party to the development of these tools, we must remain at arms-length to retain our independence, as individuals are able to file privacy complaints about the app with our Office. It is important to note that OIPC NL endorsed the province's adaption of the app; we did not approve it. Our news release on the subject is available here: https://www.gov.nl.ca/releases/2020/oipc/0903n04-2/

A Privacy Impact Assessment was conducted on the COVID Alert app at the federal level and was reviewed by the Privacy Commissioner of Canada's Office. The provincial Department of Health and Community Services did share a privacy assessment conducted on the provincial use of a federally developed portal that generates the one-time codes for the app. Both initiatives collect a minimal amount of personal information. Further, OIPC NL called for the province to evaluate both initiatives, for example examining uptake and efficacy of the app. OIPC NL also noted that "Downloading and using the app must be entirely voluntary. This is an important civil liberties issue. The OIPC encourages the provincial government to consider enacting legislation to prohibit anyone, public or private, from requiring use of the app as a condition for the provision of goods, services, entry into a premises or facility, or into the province itself."

2. Sharing of health data with health authorities and institutions

In Newfoundland and Labrador, collection of information is being conducted by the Regional Health Authorities (RHAs). Information sharing already occurs among key stakeholders (Department of Health and Community Services, NL Centre for Health Information and the RHAs) through the eHealth framework. The existing infrastructure and agreements are being leveraged for the COVID-19 response. All stakeholders as custodians as defined by the Personal Health Information Act (PHIA) and public bodies as defined by the Access to Information and Protection of Privacy Act, 2015 (AIPPA, 2015) are, as such, subject to OIPC NL oversight.

It is the understanding of the OIPC NL that retention schedules have yet to be established for some of the information collected. This has frequently been identified as a risk in the privacy assessments shared with the OIPC NL.

When it comes to health research, there is a solid regime already in place in the province. Custodians of personal health information have a review processes in place before releasing information, generally through a secondary use committee. The NL Centre for Health Information has created a Data Lab that allows approved researchers to analyze the personal health information needed for their research

without actually obtaining a copy of the information. Further (and prior to the privacy assessment), all health research conducted in the province must be approved by the Health Research Ethics Authority, as required by the Health Research Ethics Authority Act. The ethics review process involves the application of a privacy lens, but is not a substitute and occurs prior to the privacy review by the custodian of the PHI.

3. Sharing of health data with law enforcement agencies

There are two main law enforcement agencies in the province – the RCMP and the Royal Newfoundland Constabulary (RNC). The RNC is a public body subject to our oversight.

The provincial government has created a public reporting form for members of the public seeking to report fellow citizens for suspected violations of self-isolation or quarantine. It is our understanding that follow-up will be conducted either by the RCMP or the RNC, depending on location. Both law enforcement agencies have created COVID-19 units to handle such follow-up and are asking members of the public with concerns to use the form.

The provincial Public Health Protection and Promotion Act provides authority for information disclosures in public health emergencies, including disclosure for law enforcement. Further discussion of this Act is contained in a slide deck prepared by our Office in April 2020 called *Don't Blame Privacy – What to Do and How to Communicate in an Emergency*.

As the OIPC NL has oversight of the RHAs, NL Centre for Health Information and the Department of Health and Community Services, residents with concerns regarding disclosure to law enforcement are able to file a privacy complaint with the OIPC NL.

4. Sharing of health data with charitable or other similar organisations

While a resource listing is available (see, for example the resource tab at https://www.gov.nl.ca/covid-19/), the OIPC NL is not aware of any sharing of information from public bodies and custodians with support services. Impacted residents will be provided with contact information for the resource and directed to reach out themselves.

5. Handling of employee data in work-from-home / return-to-work situations

It should be noted that OIPC NL has oversight of public bodies under ATIPPA, 2015 and custodians under PHIA. The OIPC NL does not have oversight of private sector employers.

Since the public health emergency was declared, many entities have issued guidance documents regarding the new circumstances people find themselves working in. While the OIPC NL issued a privacy guidance piece called Don't Blame Privacy – What to Do and How to Communicate in an Emergency, work continues on a guidance piece dedicated to working remotely. One of the OIPC NL newsletters contained an article about working safely remotely (May edition of Safeguard). The provincial Office of the Chief Information Officer issued guidance on working remotely and the provincial government's ATIPP Office issued Guidance on Conferencing Software and Guidance for municipalities – working from home during COVID-19.

Perhaps the biggest concern of OIPC NL is the rapid pace with which changes are occurring within public bodies and custodians. While the OIPC NL appreciates the necessity of developments, like adopting virtual platforms and the creation of home offices, privacy must still be a consideration and appropriate safeguards must be in place.

While not directly related to a working from home situation, there has been one privacy complaint presented to the OIPC NL that alleged that a town Mayor had improperly disclosed information about the out-of-province travel and isolation requirements of several residents in a series of posts to a Facebook group as well as emails to Council members and Town staff. The OIPC issued Report P-2020-002 on the matter.

Again, while not directly related to working from home, several privacy breaches have been reported that are linked to a change in business process because of COVID-19. The Labour Relations Board would normally require documentation to be provided in paper form and have accepted such documentation electronically during the pandemic. A breach occurred when the entire package of documentation was provided to a third party, when only part of the information was to be shared. An RHA experienced a breach when a prescription was faxed to the incorrect number; before the pandemic, paper copies of prescriptions would have been hand-delivered. There have also been several incidents of snooping in the medical records of patients that have tested positive for COVID-19.

Canada (Québec) - Commission d'accès à l'information du Québec

1. Contact tracing and location tracking

Concerning fully automated measures: As of September 29th, the Government of Quebec announced his intention to adopt the COVID Alert app made available by the federal government of Canada. The provincial government withheld his adoption of the app at first. The initial decision was made after the Government held a public consultation on the subject, where citizens were asked to provide their opinion in a way to assess the potential adoption rate of an app, and a hearing by the Committee on Institutions of the National Assembly of Quebec, during which experts were invited to comment on the possibility of using a contact-tracing app. However, the Government changed his position after the recent resurgence of the virus in the Province.
At this time being, the app is not being fully functional. While the contact tracing function (via Bluetooth) is working, the diagnosis authentication processes still need to be put in place and implemented by Quebec public health authorities.

Concerning manual measures: The health authorities use an inquiry questionnaire [French version only]. The information collected is mainly: contact information, occupation, symptoms, locations visited two days prior to and after the appearance of symptoms, etc.). They are collected and used only to support manual contact tracing by health authorities in their inquiries surrounding COVID-19 outbreaks.

Communications are sometimes being made automatically through the use of a Web platform called Akinox which is used only in support of manual contact tracing.

Role of the Commission: The Commission is the public body responsible to oversee the carrying out of the "Act respecting Access to documents held by public bodies and the Protection of personal information" and the "Act respecting the protection of personal information in the private sector".

The Commission does not usually provide specific counsel to the government on projects prior to their implementation. However, the Commission can and sometimes does make general recommendations. Thus, the Commission published a white paper

early on during the health crisis about the use of technology in the context of a pandemic.

As mentioned earlier, the government of Quebec held public consultations throughout the summer about the possibility of deploying automated contact tracing. The Commission was invited to intervene in a special consultation on the subject by the Committee on Institutions of the provincial parliament. A brief was produced by the Commission in the wake of this consultation [French version only].

The Commission has an Oversight division that holds the power to inquire into the application of the Acts aforementioned. Should the provincial government decide to participate in the federal government contact tracing measure or to deploy its own automated or semi-automated contact tracing measure, the Commission will use its power to review this initiative in order to validate the legal conformity of the measure.

Good practices recommended by the Commission: Privacy impact assessments (PIA) are not mandatory in Quebec, but the Commission strongly recommends that they be conducted, especially in the context of contact tracing. The Commission has made available a draft version of a guide concerning PIAs [French version only].

The conducting of a PIA was one of the recommendations made by the Commission in its brief to the Committee on Institutions. Other noteworthy recommendations were:

- To establish a continuous evaluation mechanism measuring efficacy and pertinence of the contact tracing measure;
- To follow Privacy by Design and Data minimization principles in the measure's development and deployment;
- To ensure voluntary adhesion through information, transparency and conditions guaranteeing a valid and meaningful consent;
- To be fully transparent about the measure;
- To limit the uses of personal information, favoring data anonymization and a decentralized approach to data collection;
- To clearly define the objectives and permitted uses of the data, and to strictly limit access to it; and
- To ensure the temporary nature of the measure.

Considering the limits of the current provincial laws in Quebec, the Commission strongly recommended that a special and specific regulatory framework be adopted regarding an eventual contact tracing measure, thus ensuring sufficient data and privacy protection.

It is deemed important to mention that a bill aimed at improving the current provincial laws was introduced last June by the government of Quebec. It is actually under revision. The following comments pertain the actual laws and do not reflect the changes that the adoption of the bill would introduce.

2. Sharing of health data with health authorities and institutions

Public Health Act provides for some sharing of health data with authorities. The Privacy acts in Quebec also provide for some sharing of information in certain limited circumstances. Further information can be found here on the subject of data sharing between provincial health authorities in the Province of Quebec, especially in the context of a sanitary crisis.

Some of these data sharing require an agreement authorized by the Commission. One existing agreement was reassessed by the Commission and was modified to include two additional research projects aimed at fighting COVID-19.
The initial data sharing agreement was signed between the Ministry of Health and Social Services, the universal health insurance administration and a governmental research institute. In order to fulfill two additional mandates given by the Ministry, not included in the initial agreement, the research institute needed to have access to files pertaining to COVID-19 cases. The access to these files were not part of the initial agreement.

The Commission has no particular role prior to health data sharing and use between health authorities and health-related institutions (such as hospitals or social services). Authorization are provided by the general management of the institutions involved in the agreements. However, the Commission has the power to hold an investigation on its own initiative or following a complaint.

Sharing of health data to authorities and institutions others than health-related is regulated by the Act respecting Access to documents held by public bodies and the Protection of personal information. It is usually done via official data sharing agreements overseen by the Commission. The Commission must first provide a favorable opinion for the agreement to become effective. This was done in the case discussed above.

In cases implying sharing of personal health data for research projects, the Commission is involved only when personal data is to be used in a secondary project where consent cannot be obtained. In such a case, the Commission must first grant an authorization to receive communication of the data to the person or agency requesting access.

The Commission has been currently prioritizing requests concerning the sharing of health data for fighting COVID-19, but cannot provide information about these requests.

The Commission promotes the following good practices in relation to data sharing with health authorities and institutions. Any sharing of data should be done in accordance with the legislation, which usually requires written agreements. Privacy impact assessments are strongly advised, as is the revision of any research project by an ethical evaluation board. The Commission also recommends data minimization; transparency; adoption of adequate and proportionate security measures; the use of depersonalized or anonymized data whenever it is possible; destruction of data upon completion of the purpose of collection and use.

3. Sharing of health data with law enforcement agencies

The commission is currently unaware of any requirement, arrangement or plan in Québec on sharing of health data with law enforcement agencies for fighting COVID-19.

Any sharing of data should be done in accordance with the legislation, which usually requires written agreements. Privacy impact assessments are strongly advised, as is the revision of any research project by an ethical evaluation board. The Commission also recommends data minimization; transparency; adoption of adequate and proportionate security measures; the use of depersonalized or anonymized data whenever it is possible; destruction of data upon completion of the purpose of collection and use.

4. Sharing of health data with charitable or other similar organisations

The commission is currently unaware of any requirement, arrangement or plan in Québec on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

Any sharing of data should be done in accordance with the legislation, which usually requires written agreements. Privacy impact assessments are strongly advised, as is the revision of any research project by an ethical evaluation board. The Commission also recommends data minimization; transparency; adoption of adequate and proportionate security measures; the use of depersonalized or anonymized data whenever it is possible; destruction of data upon completion of the purpose of collection and use. In addition, usually data must be disposed of upon completion of the initial purpose of the collection and use.

5. Handling of employee data in work-from-home / return-to-work situations

The Commission is concerned that some private companies might have put processes and procedures in place that may prove to be disproportionate with respect to public health requirements and recommendations, e.g. symptom checks at the entries of buildings, with cameras or contactless thermometers and health status questionnaires (electronic or not); automatic contact tracing devices within the company's building; register of patrons or clients; etc.

While the Commission is not aware of any factual case of use of privacy-invading work-from-home technological devices in Quebec, they remain of concern, as are the use of electronic surveillance tools in educational environments (e.g. remote proctoring). The Commission has issued guidance on its website though a **FAQ**. (French version only) Topics covered include: general privacy principles application for employers; employers' obligations towards public health requirements; information security in the work-from-home context for employers and employees; adequate evaluation of distance learning tools from a privacy perspective; register of patrons or clients. As mentioned before, the Commission has made available a draft version of a guide concerning the conducting of a PIA. The following of the data minimization principle and the conducting of privacy impact assessments are strongly advised. The Commission reminds that any initiative must be aligned with recommendations and requirements of public health.

The Commission has been conducting inquiries related to the handling of employee data in work-from-home / return-to-work situations, but cannot comment on these issues.

Estonia - Estonian Data Protection Inspectorate

1. Contact tracing and location tracking

Following measures are adopted in Estonia:

- Voluntary contact tracing COVID app, based on Bluetooth technology, legal base is the consent, connected with the Estonian e-health system. The app does not trace contacts in personalised form. The person would never get information where and with whom he/she has had contacts;
- Voluntary manual contact tracing in case of public concerts, theatre, cinemas – collection of personal data (name, contact information) is based on consent;
- Mandatory form to be filled on the border - legal base comes from the legal act; and
- Manual contact tracing by Health Board – foreseen with legal act.

The Inspectorate had several meetings with the developers of the measures to introduce the measures. Also, the contact tracing app required an amendment to the law, which was approved by the Inspectorate.
The digital contact tracing measures are subjected to the GDPR and domestic legislation requirements, such as notification requirements regarding the improper access to data.

The Inspectorate was consulted on personal data protection related issues in the planning for and implementation of the contact tracing measures, and carries out supervisory tasks in this regard.

The Inspectorate has not published specific guidelines for the data controllers (incl. COVID apps), but the Inspectorate does have general guideline for data controllers, where all these above-mentioned principles are covered. The guideline is available only in Estonian language: https://www.aki.ee/et/isikuandmete-tootleja-uldjuhendi-veebitekst

2. Sharing of health data with health authorities and institutions

Estonia has a general e-Health system, where all the health service providers are included. It doesn't mean that every service provider has automatically an access to all the data. It is allowed only in case of actual treatment of the patient. In some cases

patient has a right to deny an access (to the doctors) to his/her health data. The diagnoses (including being COVID positive) are available in the e-Health systems, but the access to this data is for the person itself or to the doctor who has actual treatment (no matter in which hospital the doctor works).

e-Health data can be used for scientific and new-policy making researches under certain conditions (depends on a case, it needs the permission from specific ethics committee or from the Inspectorate).

3. Sharing of health data with law enforcement agencies

Estonian Health Board has a right for manual contact tracing (regulated by the legislative act) and it has a right to use professional assistance from police department. In order to provide assistance, police do not have access to the e-health system's data. The necessary information is provided separately.

4. Sharing of health data with charitable or other similar organisations

The Inspectorate is not aware of any requirement, arrangement or plan in Estonia on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

The Inspectorate is also not aware of researches based on the data received from charity organizations.

5. Handling of employee data in work-from-home / return-to-work situations

The Inspectorate has received some requests for information or clarification regarding the handling of employee data in work-from-home / return-to-work situations.

The major privacy issues identified by the Inspectorate in relation to handling of employee data in work-from-home / return-to-work situations is where employees may be asked to provide too much information.

The Inspectorate has published an information sheet to the employers about how to handle the privacy issues in case of COVID issues. It is available only in Estonian language
https://www.aki.ee/et/uudised/kas-tootajat-saab-kohustada-raakima-koike-oma-tervislikust-seisundist.

Europe - Council of Europe Data Protection Commissioner

1. Contact tracing and location tracking

The Council of Europe, based on the Headquarters' Agreement with France and on art 11 of the French law No 2020-546 of 11 May 2020, is actively cooperating with the French national authorities' endeavours to track persons who might have been in contact with an infected person.

The French law No 2020-546 empowers the French Health Minister to implement a system for the processing and sharing of health data relating to persons infected by the virus and to persons who have been in contact with them.

The information system, which is created by a Decree, is based on two tools:

- a national database called Sidep (integrated screening and prevention service) to centralise information and share it with the various health actors and practitioners;
- the Health Insurance Fund's Contact Covid teleservice to monitor patients and identify contact cases.

The system is complemented by the voluntary use of a mobile app which is built on the use of Bluetooth technology. Both measures are intended to supplement manual contact tracing.

The Data Protection Commissioner was consulted on personal data protection related issues in the planning for and implementation of the contact tracing or a location tracking measure, as well as the DPO.

The Data Protection Commissioner in consultation with the DPO issued detailed recommendations on the implementation of those measures by the Organisation. The Data Protection Commissioner has an oversight role regarding personal data processing by the Organisation also for medical purposes which he can exercise based on a complaint or ex officio.

In a joint statement published on 28 April 2020 the Chair of Committee 108 and the Data Protection Commissioner recall that general principles and rules of data protection are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health and that it is essential to ensure that data protection frameworks continue to protect individuals and that the necessary privacy and data protection safeguards are incorporated in extraordinary measures that are taken to protect public health. https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter .

Furthermore it is worth mentioning that a report entitled "Digital solutions to fight COVID-19" was published on 12 October 2020 which deals in a large extent with the issue of how personal data are processed in the 55 State Parties of Convention 108, in relation to the crisis caused by COVID-19. The report prepared by the Data Protection Unit on the basis of researches carried out by two experts builds also on contributions of State Parties and reports of media, civil society and academia. The Executive summary of the report recommends notably that:

> *"(…)*
>
> - *Exceptional measures taken by governments must be provided for by law, respect the essence of fundamental rights and freedoms and be necessary and proportionate in a democratic society.*
> - *The manner in which the health crisis has been addressed prompts a reaffirmation of the resilience of the data protection principles as a key component of the effective functioning of our democracies. The future lies in our capacity to react promptly to new challenges without undermining our core values and putting our societies at greater risk on the longer term than do the present threats we have to address."*

The report is available at: https://rm.coe.int/report-dp-2020-en/16809fe49c

2. Sharing of health data with health authorities and institutions

There is an arrangement between the Council of Europe and France to share health data with health authorities and institutions for fighting COVID-19.

The Data Protection Commissioner's role in this regard is to check complaints or ex-officio if health-related data were not shared outside of the scope of the above described arrangement.

The Data Protection Commissioner considers good practices of such sharing of health data includes prior consultation of the Data Protection Officer, the Data Protection Commissioner and the Staff Committee, having a viable legal basis for disclosing the

data, maximum transparency towards data subjects if the legal basis for the disclosure is not consent.

The health data will not be retained for research by the Organisation. French authorities might retain personal data in the public interest, but in anonymised form and with appropriate safeguards.

3. Sharing of health data with law enforcement agencies

Health data is not shared by the Organisation with law enforcement agencies for fighting COVID-19. The Data Protection Commissioner's role in this regard is to check against complaints or ex-officio if health-related data were not share with law enforcement agencies.

4. Sharing of health data with charitable or other similar organisations

Health data is not shared with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

The Data Protection Commissioner's role in this regard is to check against complaints or ex-officio if health-related data were not share with charitable or similar organisations.

5. Handling of employee data in work-from-home / return-to-work situations

The Data Protection Commissioner has not received any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

The major privacy issues identified by the Data Protection Commissioner in relation to handling of employee data in work-from-home / return-to-work situations relate to data security and the use of Video teleconferencing (VTC) tools.

The Data Protection Commissioner recommends to put in place the following measures in addressing or mitigating the privacy issues associated with the handling of employees' personal data in work-from-home/return-to-work situations: double authentication; strict access policy; periodically changing personal passwords. The Data Protection Commissioner raises regularly the awareness of the concerned entities within the Organisation of the evolving international best practices.

Europe - European Data Protection Supervisor (EDPS)

EUROPEAN DATA PROTECTION SUPERVISOR

1. Contact tracing and location tracking

Contact tracing measures:

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; and
- 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; and
- Involving data protection authorities.

On the EU Institutions' (EUIs) 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.

EDPS's engagement in the development of contact tracing measures:

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. The EDPS 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.

The EDPS has 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 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". The EDPS has 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.

The EDPS has 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.

If EUIs wish to implement contact tracing measures, the EDPS will require from them a data protection impact assessment and advocate for the minimisation of the collection of personal data, as well as the number of people having access to the data. Furthermore, the EDPS will draft general recommendations on contact tracing to all the controllers within its remit that wish to implement such measure.

Recommendations by the European Data Protection Board (EDPB)

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.

2. Sharing of health data with health authorities and institutions

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. National health authorities may request access to the information. The EUIs will abide by the applicable legislation of the Member-State where they are located, which may vary from country to country.

The EDPS, as the supervisory authority for monitoring the processing operations carried out by EUIs or bodies, will monitor their compliance when transmitting personal data to national competent health authorities.

The EDPS is following the implementation of such processing operation of data sharing with health authorities and institutions from a very early stage and have issued recommendations in that regard.

In some EU Member States, COVID-19 is a notifiable communicable disease. So the general practitioner who has made the diagnosis will report a positive case to public health authorities (including the person's name, and the public health authority will get in touch with them for contact tracing). Informing colleagues of the identity of a confirmed case: when doing manual contact tracing, public health authorities are very careful not to disclose that information. This means GDPR and the legal acts assigning these tasks to competent national authorities apply to their further processing. The competent authorities are separate controllers from the EUIs here. Retention periods,

data subject rights, etc., follow the procedures adopted by the competent authorities. The relevant national DPA supervises their compliance with the GDPR.

Regarding the data retention of health data in the public interest, the EDPB has issued specific guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. The Guidelines recommend specific guidance in relation to the processing of personal data for the purpose of scientific research, the further reuse of the data, the legal basis for the processing and the data protection principles' application. The Guidelines also focused on the issues of the exercise of data subject's rights and the issue of international transfers for scientific research purposes.

3. Sharing of health data with law enforcement agencies

There are no requirement, arrangement, or plan in the EU on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

There are no requirement, arrangement, or plan in the EU on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The EDPS has not received any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

The EUIs have had to react to the COVID-19 crisis not only in their policy roles, but also in their roles as employers. Changes in operations, such as moving the vast majority of staff to remote working have raised numerous questions on which EUIs consulted the EDPS.

The major privacy issues were:

- time constraint for the decision-making process regarding new ways of working;
- risking those parts of your organisation once starting using freely available tools that may not be in line with your EUI's IT strategy;
- to be mindful of the principle of data minimisation and avoid unnecessary sharing of personal data when managing requests for corporate devices;

- to ensure the highest data protection standards and that the processors were also complying the data protection rules;
- possible deviation from standard processes and potential inaccessibility of automated tools during telework, thus there is a higher chance of data breaches due to human error; and
- establishing new processing operations.

The EDPS, last 15th July 2020, has published a document, 'Orientations from the EDPS. Reactions of EU institutions as employers to the COVID-19 crisis', directed at EU Institutions (EUIs) compiling the advice given on questions such as teleworking tools, staff management, health data aspects and replying to data subject access requests. This document builds on the experience of the past months and addresses the issues that were raised to us or encountered by us and is still relevant because telework will most likely be a big part of the 'new normal' for the EUIs work.

The COVID-19 outbreak has forced many EUIs to switch their operation almost exclusively to telework for most of their staff. EUIs have also made other adaptations to their operations and are planning measures to protect staff and visitors upon return to the office. However, the EDPS underlined that the emergency of this situation does not mean that data protection rules applicable to EUIs can be set aside. Data protection rules currently in force within the EUIs are flexible enough to allow for various measures in order to allow business continuity of EUIs operations and the EDPS is fully aware that some adaptations resulting from an emergency situation may require some time. At the same time, there should be no doubt that the essential data protection requirements set out in Article 8 of the EU Charter of Fundamental Rights and in Regulation (EU) 2018/1725 (the Regulation), such as the **principles of accountability, data protection by design and by default, security and transparency continue to apply**. The EDPS notes that, as public institutions, EUIs have to lead by example, in order to protect the trust their staff, stakeholders, and the public at large place in them. Although EUIs are already in the process of planning a possible gradual return to the office, telework is likely to remain a big part of the new normal for near future.

Practical recommendations by the EDPS include:

- issuing clear policies on the use of private devises for teleworking;
- following the EDPS established IT governance processes as far as possible;
- to privilege the most privacy friendly tools and ensuring that they have appropriate control over how external providers will handle the data entrusted to them;
- making sure that the controller-processor agreements cover all the mandatory elements under Article 29(3) of the Regulation (EU) 2018/1725 and that when

using providers established in the EU/EEA, be sure to check if their services entail any transfers of personal data outside the EU/EEA and in that case ensure that the provider has appropriate safeguards, such as binding corporate rules;

- raising staff awareness on common data breach sources such as increasing spoofing, phishing and social engineering attacks using COVID-19 related messages; and
- handling teleworking requests to staff that has been in zones considered orange or red by the competent health authorities with restricted access to the information regarding COVID-19 cases. All the recipients apply strict measures to ensure that personal data are not accessed by anybody else. This includes the use of locked closets, encrypted email and printing with badging.

Finland - Office of the Data Protection Ombudsman

1. Contact tracing and location tracking

Contact tracing app

The Finnish Institute for Health and Welfare (THL) has produced a contact tracing app (Koronavilkku). THL acts as the controller referred to in the EU General Data Protection Regulation (GDPR) of the data processing within the application. The obligation for THL to provide the application and to act as the controller is stated in chapter 4a (temporary, valid until 31.3.2021) Finnish Communicable Diseases Act.

In addition to THL, the Finnish Ministry of Social Affairs and Health, the Social Insurance Institution of Finland (Kela) and SoteDigi Oy have participated in the development of the application. Solita Oy has provided the technical implementation of the app.

The app traces contacts. It does not track location. It allows people to participate in preventing the spread of the virus and to protect their own and others' health. Through the app, people exposed to the virus can be reached and infection chains can be stopped faster. The app is a part of the Finnish Government's test, trace, isolate and treat -strategy.

Using the application is voluntary. More information on the application and its functions: https://koronavilkku.fi/en/. See also: https://thl.fi/en/web/infectious-diseases-and-vaccinations/what-s-new/coronavirus-covid-19-latest-updates/transmission-and-protection-corona-virus/contact-tracing-app-will-help-stop-chains-of-infection.

The Finnish health officials trace contacts manually by interviewing those who have been diagnosed with the virus. The specifics of this duty are set in section 23 of the Finnish Communicable Diseases Act.

An unofficial English translate of the Finnish Communicable Diseases Act (does not include sections on the contact tracing app): https://www.finlex.fi/en/laki/kaannokset/2016/en20161227.pdf .

Engagement with the Office of the Data Protection Ombudsman

The Office of the Finnish Data Protecion Ombudsman gave an opinion during the legislative process and had conversations with the organisations that participated in the development of the application.

The legislation behind the development of the application was written taking into account the opinion of the European Data Protection Board (EDPB) on the matter: https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en .

The controller made a data protection impact assessment before the app was released. The Communicable Diseases Act also includes an obligation for the Finnish National Cyber Security Centre of the Finnish Transport and Communications Agency to review the application before its release.

The purposes for which the data can be used is defined in the Communicable Diseases Act. The data cannot for example be used for law enforcement purposes. The application is available temporarily (until March 2021) and all data will be deleted at the latest accordingly.

The Office of the Finnish Data Protection Ombudsman acts as the data protection supervisor referred to in the GDPR and can use its powers accordingly.

2. Sharing of health data with health authorities and institutions

According to the Communicational Diseases Act Chapter 4 all physicians and dentists have a duty to notify the National Institute for Health and Welfare of suspected or diagnosed cases of generally hazardous or monitored communicable diseases. There are also other obligations to provide information to other health officials. See Chapter 4 of the Communicational Diseases Act.

The use of patient data for scientific purposes is regulated in the Act on the Secondary Use of Health and Social Data. See https://stm.fi/en/secondary-use-of-health-and-social-data and in more detail: https://stm.fi/en/frequently-asked-questions-about-the-act-on-secondary-use-of-health-and-social-data .

In this regard, the Office of the Finnish Data Protection Ombudsman acts as the data protection supervisor referred to in the GDPR and can use its powers accordingly.

See also EDPB statement on the data protection impact of the interoperability of contact tracing apps:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf .

3. Sharing of health data with law enforcement agencies

The purposes for which the data can be used is defined in the Act. The information cannot be used for example for law enforcement purposes.

4. Sharing of health data with charitable or other similar organisations

The Office of the Data Protection Ombudsman is aware of some projects that have included sharing data to these organisations. Patient data can be disclosed to a third party in certain situations defined specifically in relevant legislation, for example when a patient consents to sharing the information. In this regard, the Office of the Finnish Data Protection Ombudsman acts as the data protection supervisor referred to in the GDPR and can use its powers accordingly.

5. Handling of employee data in work-from-home / return-to-work situations

Good practices promoted: See the act on the Protection of Privacy in Working life, unofficial English translation
https://www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf

Gabon - National Commission for the Protection of Personal Data

1. Contact tracing and location tracking

Our jurisdiction has not adopted a digital method of contact research or a tracing method. Our authority has also not been contacted in regard to personal data protection related issues of contact tracing or location tracking measures.

Our authority generally enforces the law on the use of GPS and the installation of surveillance cameras by providing users with a document containing standards of good practice.

2. Sharing of health data with health authorities and institutions

Steps to establish health data sharing mechanism with health authorities and institutions are underway.

To date, the Ministry of Health and our Commission are working together to proceed with the regularisation of the relevant public acts that were quickly adopted at the outbreak of the pandemic. Thus, in general interest, the Government has set up a branch of the Ministry of Health called the Steering Committee (COPIL) in charge of the response plan against the COVID-19 pandemic. This Committee is responsible for ensuring urgent measures being taken during the Extraordinary Council of Ministers meeting to prevent the spread of the virus:

- Asepsis measures for all business sectors;
- Patient care in hospitals; and
- Mass screening.

The types of health data that will be shared are:

- confirmed diagnoses of Covid-19;
- complications due to Covid-19; and
- the underlying pathologies.

The data will be shared via a secure virtual private network (VPN).

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in your jurisdiction on sharing of health data with law enforcement agencies for fighting COVID-19, though the law provides for an exception to the principles: measures are taken by the Government (COPIL) of a health security system on any person wishing to travel nationally and abroad by issuing directly to that person a certificate stating that he or she is negative to the Covid-19 test.

4. Sharing of health data with charitable or other similar organisations

Our authority has not yet set up a mechanism for sharing health data with charities or similar organisations.

5. Handling of employee data in work-from-home / return-to-work situations

There is a significant data flow that runs via videoconference. This technology has very quickly transformed all sectors: schools, universities, public administrations, etc. Teleconference records conversations and stores images. This raises the issue of confidentiality. Our authority intends to regulate the duration of the storage of these data and their purpose, with strict respect for privacy.

Georgia - State Inspector's Service

1. Contact tracing and location tracking

The 'Stop Covid' App

In April 2020, the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia launched a mobile application - "Stop Covid". The app allows users to find out if they have been in contact with a person infected with Covid-19.

The purpose of the mobile app is to detect and prevent Covid-19 as early as possible. It allows the user to find out if they have been in contact with a person infected with Covid-19 (means a person who has downloaded and activated the same application). The app uses Bluetooth, location and Google Nearby technologies to determine which mobile phones were in close contact with each other.

Information about the interaction between the users of the application (contact date, certain duration (more than 15 minutes) and distance (less than 2 meters)) is stored locally on the relevant mobile device, in the mobile phones of the contacted users. If any of them are confirmed by Covid-19, by clicking on the appropriate button in the app, they can notify those who interact with it about the infection. The notification procedure is as follows: When you press the button, a form for entering a mobile phone number appears. After entering the phone number in the form, a one-time code (PIN) is sent to the phone number in the form of a short text message, which must be indicated in the application for confirmation. Phone number is checked by National Center for Disease Control and Public Health in the unified database of Covid-19 infected people. In case of confirmation of the infection of the owner of the indicated telephone number, the message made by the user in the application will be confirmed. After confirming the phone number, the user agrees or refuses to share information about their contacts within the last 5 days. As a result, those who have been in close contact with the infected user's mobile phone for the last 5 days are sent a warning with the relevant instructions through the application.

Engagement with the State Inspector's Service

The application was reviewed by the State Inspector's Service, which revealed the relevant shortcomings and challenges. Relevant recommendations were provided by the State Inspector's Service. The following challenges have been identified:

- It is advisable to make the app and its privacy policy more transparent to users. It should provide the most detailed information to the customer.
- The possibility of effective realization of the data subject's rights must be ensured. The data subject must be able to refuse the consent he has given. Data subjects should have the right to request the deletion of their personal data.
- Data Processing Objectives and the storage period - Data may only be stored for the period necessary to achieve the purpose of the data processing. The storage period of the data collected through the application is 3 years. According to the Ministry, this term is conditional and can be revised. Accordingly, the specific purposes of data processing should be specified and the relevant data retention period should be determined.
- Periodic change of unique user code - The unique user code of the application, which is then used to fix close contacts is unchanged (changes only when the application is deleted and re-downloaded by the user from the mobile phone). In order to maximize the depersonalization of data subjects, it is desirable that the unique codes used by the application do not remain unchanged and change periodically, randomly.
- Access to the Software Code of the Application - In order to ensure the transparency of data processing through the application and the compliance of this process with the law, it is desirable that the application code of the application be made available to the public.

2. Sharing of health data with health authorities and institutions

Order of the Minister of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia regulates data sharing between health authorities and institutions. According to the order, information about infected persons should be recorded in a special module. The same order determines the categories of personal data and the periods for data sharing.

The State Inspector's Service supervises the legality of such data processing. The State Inspector's Service issued recommendations regarding the data processing during a pandemic. Besides, the Service advises public and private organizations on specific data processing processes.

3. Sharing of health data with law enforcement agencies

The resolution of the Government of Georgia On Isolation and Quarantine Rules and the resolution of the Government of Georgia on Action to prevent the possible spread of a new coronavirus in Georgia and cause a new coronavirus to approve a contingency response plan regulate the sharing of health data with law enforcement agencies. For example:

- In order to transfer a person to the quarantine area Revenue Service (also responsible for Customs), National Center for Disease Control and Public Health and Center for Emergency Coordination and Emergency Assistance are authorized to provide the Ministry of Internal Affairs of Georgia with information about the person to be quarantined (name, surname, personal number and contact information).
- In order to control the observance of the conditions of isolation by a person in self-isolation, National Center for Disease Control and Public Health sends information about a self-isolated individual (name, surname, personal number, contact information and self-isolation / residential address) to the Ministry of Internal Affairs of Georgia.

The State Inspector's Service was consulted before drafting the regulation.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Georgia on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The State Inspector's Service has not received any complaints related to the handling of employee data in work-from-home / return-to-work situations.

The major privacy issues identified by the State Inspector's Service in relation to handling of employee data in work-from-home / return-to-work situations concerns the collection of employer data about his/her and his/her family members: contacts, travel history, health data. State Inspector's Service issued recommendations on "personal data protection in the course of fight against Covid-19", which included recommendations on Processing the data of employees by employer organisations (https://personaldata.ge/en/press/post/6349).

Germany - The Federal Commissioner for Data Protection and Freedom of Information (BfDI) [25]

1. Contact tracing and location tracking

Measure #1) Digital measure: Corona-Warn-App

Development:

- Google/Apple Exposure Notification Framework (Bluetooth) based contact tracing application.
- Published by the Robert Koch-Institute, Germany's national health authority.
- Developed by SAP & Deutsche Telekom on behalf of the Federal Government.
- The Corona-Warn-App is intended to supplement manual contact tracing.
- The Corona-Warn-App itself does not collect additional data so data collection is limited to the minimal dataset as required by the GAEN.
- The measure is not clinically relevant or necessary. (Note: Measures aiming at containment generally cannot be clinically relevant.)
- The data is used to trace contacts and inform users about potentially associated risks.
- According to the GAEN approach data regarding contacts is not disclosed while pseudonymous data regarding users with identified infections is disclosed publicly.
- The use of the Corona-Warn-App in Germany is voluntary and based on consent. The federal government publicly expressed its position that use of the App should in any case be voluntary. There have been isolated remarks about an obligation to use the App. However these neither lead to broader public discussion of this topic nor was this placed on the governments agenda.

Engagement with the BfDI and privacy protection:

- The Federal Commissioner for Data Protection and Freedom of Information (BfDI) has accompanied the development process in an advisory manner. The working relationship has been constructive.

[25] In Germany responsibility for Data Protection Supervision is shared between the Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – BfDI) and the Supervisory Authorities of the federal states, the so-called "Länder". Measures and recommendations described in this chapter mainly reflect the BfDI´s view.

- The Federal Commissioner for Data Protection and Freedom of Information (BfDI) is the DPA responsible for oversight of the Robert Koch-Institute (publisher of the Corona-Warn-App) and has accompanied the development process in an advisory manner. The BfDI does/did not develop, distribute, promote or operate the Corona-Warn-App or (parts of) its infrastructure.
- Accompanying to the development of the Corona-Warn-App a DPIA has been conducted by the developers.
- Developers have addressed matters of data security in cooperation with the Federal Office for Information Security.
- Notification requirements regarding the improper access to data apply according to the regulations of the GDPR (especially Article 33).
- The data controller will have to conduct a thorough evaluation of the measure in due time. The BfDI (responsible DPA) will review the evaluation results and may take further measures.
- Penalties regarding the improper use and access to data apply according to the regulations of the GDPR.
- According to current planning the digital measure is temporary and will ultimately end whenever Google/Apple see fit as there is no legally possible way to force users to uninstall the Corona-Warn-App from their devices. So the measure will terminate whenever the GEAN service terminates and the App technically stops collecting data. As a remediation the controller / publisher may decide to unilaterally deactivate the backend infrastructure which would render the App practically useless. As previously stated there is no legally possible way for the publisher / data controller to delete the Corona-Warn-App from users devices even if it is no longer required.

Good practices recommended by the BfDI:

- Development of the contact tracing application in a transparent open source process including public release of the data protection documentation (especially DPIA) has proven valuable in terms of user acceptance.
- As required by the GDPR a privacy assessment should be and has been conducted on behalf of the data controller.
- As required by the GDPR data minimization should be and has been considered by the data controller.
- As required by the GDPR usage limitations and transparency requirements should be and have been considered by the data controller.
- Generally speaking - adherence to the rules of the relevant DP regulatory framework seems to be a pretty straightforward approach and for many aspects will substitute the additional development of good practices.

- Besides the statistical comparison of promotionally effective but actually meaningless numbers (e.g. number of downloads in total) there is no legal possibility to monitor the efficacy of a contact tracing measure in a decentralized approach based on a proper implementation of the GAEN approach, as all relevant data is minimized, pseudonymous, statistically obfuscated by additionally invented values, and is likely not to correlate to findings derived from manual contact tracing, since notifying contacts not accessible to the manual approach is the whole point of the effort.
- Relevant publications that have been developed by the EU DPAs (including BfDI) as members of the EDPB can be found here:
    - https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en
    - https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en
    - https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/statement-data-protection-impact-interoperability-contact_en
- Information about the Corona Warn-App: https://www.coronawarn.app/en/ (See section “Data privacy and security”)

Measure #2) Collection of address-information e.g. in restaurants, cinemas, at meetings and events.

- The data are recorded and on demand handed out to the local health authority to support contact tracking.
- Owners of restaurants, bars or other venues, which are accessible to the public, are encouraged not to use lengthy lists containing contact details of customers, but to rather use a single sheet for each customer to collect their contact details.
- In any case, such files of contact data need to be deleted or destroyed as soon as they are no longer necessary.
- Access of public authorities – health authorities or law enforcement authorities – to these contact data files must be restricted to purposes where processing of such data is necessary for fighting the Covid-19-pandemic or for another legitimate reason.
- This measure is based on laws of the Bundesländer.

2. Sharing of health data with health authorities and institutions

Laboratories, Doctors and Hospitals are obligated to inform the local health authorities about Covid-19 infections and positive test results and provide information

on the case including diagnosis and date of infection. The local health authority has to transmit the data to the federal health institution Robert-Koch-Institut.

Robert-Koch-Institut processes the data for reporting, monitoring, research and in order to develop new measurements for fighting Covid-19. So far is being kept as long as necessary. Anonymisation takes place as soon as possible.

BfDI accompanies the development and installation of the electronic reporting system (DEMIS Deutsches Elektronisches Melde- und Informationssystem für den Infektionsschutz) in an advisory manner.

As required by the GDPR a DPIA should be conducted on behalf of the data controller. Encryption and pseudonymization are obligatory.

Relevant publications that have been developed by the EU DPAs (including BfDI) as members of the EDPB can be found here:

- https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en
- https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en
- https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/statement-data-protection-impact-interoperability-contact_en

3. Sharing of health data with law enforcement agencies

There is a variety of arrangements in Germany regarding the processing of health data by law enforcement agencies. The same applies to regulations regarding the deletion of data. It is still subject to discussion to what extent law enforcement authorities can rely upon general rules for the collection of data. In addition, different provisions in the federal states (“Länder”) need to be considered.

First, it should be noted that in Germany not one single law enforcement agency is responsible for the measures taken in relation to COVID-19. The Federal Police (Bundespolizei) acts at the federal level. For instance, this concerns measures at borders. In addition, the police forces of the federal states (the so called “Länder”) are competent in the states. Due to this, there are several arrangements in Germany.

In general, law enforcement agencies in Germany have the right to conduct investigations (§§ 161, 163 StPO) and, subject to further conditions, the right of seizure (§§ 94, 98 StPO). According to these general clauses, investigations of different

types and seizures may be allowed. Therefore, the processing of health data by law enforcement agencies is not excluded in principle.

With regard to the collection of data from the private sector, a distinction must be made between a transfer of data by the body providing the information (company) and data retrieval by the body requesting the information (public prosecutor's office/police). For each collection and transmission of data, a separate but corresponding legal basis is required. In general, it can be said that the transmission of company data for the purpose of criminal prosecution, even if it is a case of a change of purpose, is possible if criminal acts are to be investigated or for the safeguard of state or public security. However, the rules applicable to each individual case must be considered.

With regard to COVID-19, the German federal states have issued specific legal regulations. In some cases, it is explicitly stated that the police is responsible for supporting the health authorities. In other cases, police authorities have an urgency jurisdiction in the event of violations of public safety. This also includes violations of the above-mentioned regulations.

In this regard, the Federal Commissioner for Data Protection and Freedom of Information is responsible for supervising federal authorities. This also includes the Federal Police. Supervision of the police forces of the federal states and the private sector is the responsibility of the Data Protection Commissioners of the Länder. Within the respective area of responsibility, compliance with the applicable regulations is monitored. In addition, the supervisory authorities monitor the legislative process.

4. Sharing of health data with charitable or other similar organisations

There are no requirement, arrangement or plan in Germany on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

On the part of the BfDI the lack of appropriate IT equipment was often noted. Here the focus was particularly on the problem of using personal hardware and software. The BfDI views this critically when processing employee data. In addition, the handling of paper-based personnel (Human Resources / Staff) files was discussed as a problem. In this regard, the supervised institutions were informed that the data protection regulations with regard to personnel (Human Resources / Staff) files were still valid under the current situation.

The following recommendations for action were made:

- the agreement and observance of access possibilities of the employer and his data protection officer as well as the competent data protection supervisory authority to the teleworking station and the IT facility for control purposes, taking into account Article 13 (Inviolability of the home) of the Grundgesetz (Basic Law for the Federal Republic of Germany);
- the regular instruction of the participating persons about the obligation and compliance with data protection regulations and principles;
- transport of paper documents in courier folders in lockable cases with two combination locks;
- keeping a register of the files carried and returned;
- having a separately lockable office room in the private residence;
- the sealing of documents at the work place at home;
- no disposal of documents at the work place at home;
- the exclusive use of hardware components approved for identification and authentication with the company's network;
- the hardware and software encryption;
- the use of passwords through a three-level password system;
- the logging of the accesses with preferred evaluation;
- the evaluation of the log files, particularly with regard to private use;
- no use of printers at the work place at home;
- the physical and logical blocking of USB accesses and other connections at computers or devices provided by the employer; and
- the use of visual protection sheets on the displays or monitors, if structural conditions make this necessary.

For further information we refer to the brochure "Teleworking and Mobile Working", which contains information on how to implement data protection regulations. This brochure is available here:
https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html.

The responsible departments of the BfDI, so far, are not aware of any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

Gibraltar - Gibraltar Regulatory Authority (GRA)

1. Contact tracing and location tracking

In Gibraltar, HM Government of Gibraltar's Digital Services Team in collaboration with the Gibraltar Health Authority ("GHA") developed a mobile application for contact tracing (the "App"), as a direct response to the current Covid-19 pandemic. The App uses Bluetooth-based technology on your mobile phone to exchange digital handshakes with the mobile phones of other App users who have been in close contact with you. Close contact consists of another App user who has been within 2 metres of an infected person for 15 minutes or more.

The App will consist of anonymous processing, by assigning all mobile phones that download the App a pseudo-random identifier, so that individuals are never identifiable. In this way you will never know who has tested positive, only that you have been in close contact to someone who has tested positive.

The App states that it does not collect personal data from its users. It simply records basic anonymous metrics to measure the usage of the App and the number of exposures notified. Any anonymous digital handshake exchanged by mobile phones are automatically deleted from the App user's device after the expiry of 14 days.

Downloading the App is completely voluntary.

Further manual measures including potentially sharing contact information (such as name, and contact telephone number) to the local health authority in certain circumstances. For example, Section 12 of the Civil Contingencies Emergency (Coronavirus) (Businesses And Restrictions) Regulations 2020, includes the following requirements for restaurants cafeterias and bars wishing to obtain a permit to open:

(a) "keep a daily list of the name and contact telephone number of all the customers who have booked a table at the restaurant or cafeteria;

(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."*

Regarding privacy, it is understood that the developers carefully considered guidance issued by the GRA together with information published by the European Data Protection Board. The GRA understands that the App does not store personal data from its users. Further, as highlighted above, any anonymous digital handshake exchanged by mobile phones are automatically deleted from the App user's device after the expiry of 14 days. Users may install or delete the App at any time.

The GRA published guidance but was not involved in the organisation or planning of contact tracing arrangements. The GRA has published the following Guidance Notes:
COVID-19: Contract Tracing & Location Data (click here)

This document provides 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.

COVID-19: Temperature Checks (click here)

In this document the Information Commissioner identifies that there may be legal grounds for employers to check the temperature of their employees and for the authorities to carry out temperature checks at Gibraltar's entry and exit points.

2. Sharing of health data with health authorities and institutions

Please refer to the above section relating to the Contact Tracing App as well as the manual measures identified.

As mentioned above, the GRA published relevant guidance in an attempt to promote good practices in relation to data sharing with health authorities and institutions. In addition, the GRA has also issued ad-hoc advice to organisations approached by the local health authority requesting information, advising that in certain circumstances, requests for information by the health authority were not justified as less intrusive measures were available. Further advice on good practice was published on the website: https://www.gra.gi/data-protection/data-protection-and-coronavirus-what-you-need-to-know

The GRA is currently looking to update its code of practice on data sharing. However, the existing code of practice in its current form provides useful guidance on data sharing. The code of practice, can be found on our website (https://www.gra.gi/data-protection/documents/codes-of-practice/data-sharing-code-of-practice).

3. Sharing of health data with law enforcement agencies

NIL.

4. Sharing of health data with charitable or other similar organisations

NIL.

5. Handling of employee data in work-from-home / return-to-work situations

The GRA established that data protection is not a barrier to increased and different types of homeworking and noted that, during the pandemic, employees may work from home more frequently than usual and use their own device or communications equipment. The GRA encouraged that employers consider the security measures that are appropriate for homeworking.

The Information Commissioner recognises the unprecedented challenges people are all facing during the COVID-19 pandemic, and understands that, in the current climate, there may be a need to share information quickly, or to adapt the way work is conducted.

In view of the above, the GRA issued a Press Release titled "Data protection and coronavirus: what you need to know" which can be accessed here. In addition to this, a social media campaign (accessed here) was also published on the GRA's social media platforms over a period of 6 weeks. Guidance on data security is available here.

To date, no complaints related to the handling of employee data in work-from-home / return-to-work situations have been received.

Hong Kong, China - Office of the Privacy Commissioner for Personal Data (PCPD)

1. Contact tracing and location tracking

The Government of the Hong Kong Special Administrative Region (Government) has introduced the mandatory use of an electronic wristband (using Bluetooth Low Energy (BLE) technology) together with a "StayHomeSafe" mobile app for those under compulsory home quarantine order.

The mobile app collects wireless communication signals (e.g. Wi-Fi, mobile networks, GPS signals, etc. together with the Bluetooth signal of the electronic wristband), and their respective strengths in the surrounding environment but not geo-location data. On activating the app, person under quarantine is required to walk around his/her dwelling place for one minute. During this process, the specific signal patterns and strength of his/her dwelling place as well as the Bluetooth signal generated by his/her paired electronic wristband, will form the "profile" of wireless signals of the quarantined person's location. It is like setting up an electronic fence (a kind of "geo-fencing" technology) and any attempt to move away from the designated location will result in change of the signals "profile" and the data will recorded in the mobile app. Data analytics of signal changes are being conducted for continuous monitoring during the quarantine period to assess if the quarantined person is staying at the designated place under the quarantine order.

Surprise video calls are made to the person under quarantine and the app will also randomly request the quarantined person to scan the QR code on his/her electronic wristband as an additional spot check measure. If the quarantined person is suspected to have left the designated place without permission, the Government will take further actions, such as conducting spot checks, making a prosecution or issuing a wanted warrant.

The detection and analysis of environmental signals do not involve collection of personal data and the actual whereabouts of the individual. The app will not read any information in the user's smartphone as well. This measure is a privacy-friendly measure that does not collect unnecessary data or excessive personal data.

The electronic wristband and "StayHomeSafe" mobile app were developed by the Office of the Government Chief Information Officer (OGCIO) together with a local tech startup adopting the above "geo-fencing" technology researched and developed by a local university. The PCPD had been consulted before the mobile app was rolled out. The PCPD provided observations to the OGCIO while maintaining our independent regulatory function. The PCPD emphasized to OGCIO the need to be transparent and explainable such that the users of the application would clearly know what kind of data would be collected and how the data would be used.

A privacy by design approach was taken to develop the "StayHomeSafe" mobile app, which does not collect geo-location data and does not have access to information stored in user's smartphone. Data is stored securely and encrypted during transmission.

Another digital measures deployed is the Major Incident Investigation and Disaster Support System (MIIDSS), usually referred to as the "supercomputer". MIIDSS is deployed to assist in tracing those people suspected of having close contact with COVID-19 patients using big data analytics. It is a system used by the Hong Kong Police Force for data management and big data analysis. According to the Hong Kong Police Force, it has utilised MIIDSS to assist the Centre for Health Protection in tracking down carriers of the virus, with the aim to sever transmission pathways as early as possible. Up to 2 June 2020, over 19,000 sets of data had been uploaded to the system, which had facilitated the investigation into 14 transmission groups as well as the in-depth follow-up on over 1,350 confirmed patients and the people they had met. By tracing the places they had visited and their activities, 122 hidden contacts were identified.

While it is not compulsory for data controllers or developers to consult the PCPD before implementing any measures which have implications on personal data privacy, the Government has actively engaged with the PCPD and consulted it on the personal data privacy issues arising from those measures.

The PCPD recommends the following good practices on the use of digital contact tracing measures:

- Data users must adhere to the principles of necessity and proportionality, and must not unduly derogate from their responsibilities in protecting personal data. Only minimum, necessary, non-excessive personal data should be collected, and the purpose of their collection should be directly related to their functions or activities (e.g. ascertaining the health condition of the data subjects). The personal data shall only be used for specified purposes and shall not be used for any new purposes unless prescribed consent from data subject is obtained.

- The monitoring measures should be time-bound and continue only for as long as it is necessary to address the COVID-19 pandemic.
- Data shall not be kept for indefinite period. Data users shall delete the data that is no longer necessary.
- Personal data collected must be protected with appropriate safeguards and security measures. This would include, but not limited to, (1) proper access control restricting who can access the data, such as strong passwords before retrieving any data inside in the system and access to data by designated staff only for a legitimate purpose; (2) encrypting the data; and (3) locking the cabinet(s) storing the physical files. Proper logs of which staff members in custody of the collected data should be updated on time. Transfers and movements of the collected data should also be clearly documented.
- Transparency and explainability are always the key principles to build trust when deploying new technologies (such as big data analytics and the use of AI) that may impact people's rights and freedoms. Data users should be transparent about and explain clearly and comprehensively the rationale for the measures as well as the science behind the technology, to the public and in the media. This can be done by way of comprehensive and clear privacy notices, policies and practices. Any significant concerns raised by the public regarding privacy should be adequately addressed – informing and educating the public will enable individuals to make informed decisions and choices and hold the authorities accountable.

2. Sharing of health data with health authorities and institutions

The requirements on sharing of health data with health authorities and institutions for fighting COVID-19 in Hong Kong are stipulated under Prevention and Control of Disease (Disclosure of Information) Regulation (Cap. 599D, Laws of Hong Kong).

Any data relevant to the handling of the public health emergency and relevant to the identification and tracing of any person who may have been exposed to the risk of contracting COVID‑19, including but not limited to (a) the places where the person has been to; (b) the medical history of the person; or (c) any contact between the person and other persons, may be shared. It would be an offence for giving false or misleading information. This Regulation expires at midnight on 31 December 2020. In addition, only fully anonymized health data can be retained for research purposes.

Any person shall comply with the directions of the Centre for Health Protection of the Department of Health to provide information relevant to the handling of the public health emergency and relevant to the identification and tracing of any person who may have been exposed to the risk of contracting COVID‑19.

The requirements under these regulations are outside the PCPD's regulatory ambit. Nonetheless, the PCPD provided some general observations on the legitimacy of sharing health data with health authorities through various media statements, advised the health authorities to adhere to the data protection principles, and recommended the following good practices in relations to data sharing with health authorities and institutions:

- Sharing only necessary but not excessive data
- Be transparent and explainable of what data will be shared and how the data will be shared
- Deleting data that is no longer necessary
- The sharing should be time-bound and continue only for as long as it is necessary to address the COVID-19 pandemic
- Having adequate security measures in place to keep the data secured
- No further sharing of the data unless for same purposes or required under the laws

3. Sharing of health data with law enforcement agencies

There is no statutory requirement which mandates sharing of COVID-19 related health data with law enforcement agencies. That said, sharing of health data with law enforcement agencies may happen if the sharing of personal data is for protecting the health of individuals and public health at large. Sections 59(1) and (2) of the Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong) provide that the use of individuals' health data, identity data and location data may be exempt from the application of the use limitation principle if compliance would be likely to cause serious harm to the health of the individuals concerned or other individuals. In other words, any breach of the general rule on the use of personal data without the data subjects' consent may be defended by demonstrating that the use of the personal data is for protecting the health of individuals and public health at large.

4. Sharing of health data with charitable or other similar organisations

N/A for Hong Kong.

5. Handling of employee data in work-from-home / return-to-work situations

The PCPD issued some practical tips for the employers and employees when collecting and providing personal data to combat the COVID-19 pandemic (see https://www.pcpd.org.hk/english/media/media_statements/press_20200330.html).

The major concerns for employers are (1) whether they are permitted to collect health data about their employees to help monitor and prevent the spread of the virus in the workplace and the wider community; and (2) whether they can disclose to other staff or the management company of the office buildings the personal data of employees who are confirmed COVID-19 cases.

Employers must follow the general rule that the measures taken to collect data should be necessary, appropriate and proportionate. They should seek to process the relevant data in an anonymised or de-identified way. A self-reporting system is preferred to an across-the-board mandatory system where health data is collected indiscriminately. Least privacy intrusive measures should be preferred. For example, for the sole purpose of temperature checking before entry into buildings or offices, the PCPD would generally consider that the use of cameras with facial recognition technology is unnecessary and disproportionate as there are less privacy intrusive alternatives available.

Personal data collected by employers for fighting COVID-19 must not be used or disclosed for other unrelated purposes, unless express and voluntary consent is obtained from the individuals concerned or exemptions under the PDPO apply. For the purpose~~s~~ of protecting public health, it is generally acceptable for employers to disclose the identity, health and location data of individuals to the Government or health authorities solely for the purposes of tracking down and treating the infected, and tracing their close contacts when pressing needs arise. In these circumstances, exemptions under the PDPO may be invoked. Section 59(1) of the PDPO provides for situations where the use of personal data relating to the health of the data subjects may be exempted from the application of use limitation principle if the application of such rule would cause serious harm to the health of the data subjects or any other individuals. In other words, any breach of the general rule on the use of data without consent may be defended by demonstrating that the use of the data is for protecting the health of individuals and public health at large. In particular, section 59(2) of the PDPO states that in circumstances where the application of the use limitation principle would be likely to cause serious harm to the physical or mental health of the data subject or any other individuals, personal data relating to the identity or location of the data subject may be disclosed to a third party without the consent of the data subject.

However, under most circumstances, disclosure of the name and personal particulars of an infected employee to other employees, visitors and the property management office, etc., will generally not be considered as necessary or proportionate.

Regarding retention of data, employers shall permanently destroy the personal data collected for the purposes of fighting COVID-19 when the purpose of collection is fulfilled, such as when there is no evidence suggesting that any employees have contracted COVID-19 or have close contacts with the infected after a reasonable period of time.

Adequate data security safeguards (e.g. storing the data in a locked cabinet, encrypting the data and only allowing authorised personnel to have access to the data) shall also be in place for storage and transmission of medical or health data because medical and health data is more sensitive and a breach of health data may cause significant harm to the individuals concerned.

The PCPD received enquiries from employers on whether they could collect extra personal data (such as health data) from their employees during COVID-19 and whether they could disclose details of confirmed cases to other employees, customers and/or property management. It also received enquiries from individuals who asked if it was mandatory to provide their health data to their employees. The PCPD provided observations and guidance to them.

Japan - Personal Information Protection Commission Japan

1. Contact tracing and location tracking

An app named COCOA (Contact-Confirming Application), developed by the Ministry of Health, Labor and Welfare (MHLW), is rolled out in Japan (The app has been developed based on application programming interfaces (APIs) offered by Apple and Google). The app records and stores the history of contacts of more than certain level between Apps users (so-called "close contact"), using Bluetooth of mobile terminals and to warn close contacts of the said user promptly using such records in the case where Apps users are diagnosed as being infected. The app notifies the users of close contact with COVID-19 positive users to help seek instructions from the public health centres, and enables subsequent actions to be taken.

No personal information such as names, contact details (phone numbers etc), or location information is collected.

The records of "close contact" are stored within each user's mobile device, and will not be sent out to the third party nor stored at the central server.

When a user is tested positive for COVID19, he/she can register the Processing Number of their test results issued by the public health centres in the app. The app then notifies the user who were in close contacts. The app is not intended to complement manual contact tracing. The use of the app and registering the Processing Number of the user's test result are on voluntary basis.

In developing the contact tracing app, the PPC Japan published its views on the contact tracing apps, prior to its development. The PPC Japan also took part in the Experts' Meeting on Contact Tracing Apps as an observer and made necessary interventions. The PPC Japan 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 opinion representing a view to utilize such Apps, paying attention to the balance between the demands for securing the rights and interests of individual related to personal information and those for public policy use as a countermeasure for infectious diseases.

The Experts' Meeting on Contact Tracing Apps drafted the specification document of the app, and made assessments on its privacy and security aspects. In doing so, the PPC's views on the contact tracing apps were taken into account.

The members of the above said Meeting consisted 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.

The Experts' Meeting on Contact Tracing Apps made assessments of the app on protection of personal information and privacy. The app does not collect information such as names, contact details (phone numbers etc.) and location information (The app has been developed based on application programming interfaces (APIs) offered by Apple and Google). The use of the app is on voluntary basis, and the consent pertaining to the user of the app can be retracted at any time by deleting the app from mobile device, and all stored information will be irrecoverably deleted.

Information pertaining to contact with other App Users recorded in the mobile devise are recorded in an encrypted state and are automatically invalidated after 14 days.

The PPC Japan published its views on the use of contact tracing app on its website and advised the business operators to inform the users that they do not obtain unnecessary data in relation to the utilization purpose and it does not provide the data to a third party: https://www.ppc.go.jp/files/pdf/information_20200501.pdf.

In the interest of maintaining transparency and accountability, MHLW, the main developer of the app, has published on its website the terms and conditions of use, privacy policy, specification document of the app, and notes on the specification document: https://www.mhlw.go.jp/stf/seisakunitsuite/english_rk_00031.html; https://www.mhlw.go.jp/stf/seisakunitsuite/english_pp_00032.html.

2. Sharing of health data with health authorities and institutions

Under the Act on the Protection of Personal Information, obtaining in advance a principal's consent is essential when utilizing personal information for the purpose which is different from the utilization purpose originally notified to a principal, or to provide it to a third party including a central government organisation.

However, the following cases are considered to be exceptions (APPI Article 23(1));

1. cases based on laws and regulations;

2. cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent;
3. cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent; or
4. cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs.

The results that the public health centres or medical institutions obtained through PCR test, Antigen test, active epidemiological investigations/surveys such as manual contact tracing, and etc., are shared with the public health institutions in accordance with the Act on the Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases.

In addition to the above, smooth transfer of patient's medical data amongst the medical institutions is enabled in accordance with the Act on the Protection of Personal Information etc.

The data obtained by the public health authorities through investigations/survey which is based on the Act on the Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases are stored and utilized within the scope of specified utilization purpose. These data are controlled properly, taking necessary safety measures, in accordance with the Act on the Protection of Personal Information Held by Administrative Organs.

The role of the PPC in regard to such data sharing is to ensure the proper handling of the personal data in accordance with the Act on the Protection of Personal Information.

In order to clarify that providing information to public health centres to enable them to carry out epidemiologic investigations/surveys such as manual contact tracing, based on the Act on the Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases, does fall under the category of exemption to the principle of consent of the individual as provided in the Act on the Protection of Personal Information, the PPC Japan has published the Q&A and revised the guidelines accordingly.

The PPC Japan has also published a Q&A, in collaboration with the health authorities, on the handling of the Act on the Protection of Personal Information when sharing personal information amongst the health care facilities in dealing with COVID-19 cases.

3. Sharing of health data with law enforcement agencies

Please refer to section 2 for the general requirements on data sharing and the Act on the Protection of Personal Information.

The PPC Japan set the Guidelines and the Q&A of the Act of the Personal Information Protection Act which provide interpretation of the provisions on providing personal data to law enforcement agencies.

In addition to this, the information on the provisions on proper handling of personal data in the interest of further preventing the COVID-19 is made available on the PPC Japan's website.

4. Sharing of health data with charitable or other similar organisations

Please refer to section 2 for the general requirements on data sharing and the Act on the Protection of Personal Information.

5. Handling of employee data in work-from-home / return-to-work situations

Many of the business operators seem not to have enough understanding about when a consent of the principal is needed in the event of employees being tested positive with COVID-19, under the Act on the Protection of Personal Information.

In addition, it does not seem to be widely understood that sensitive personal information of the employees can be handled even working from home as long appropriate safety measures are taken against any possible leakages etc.

The PPC Japan tries to raise awareness of proper handling of personal information by providing examples when a consent of the principal is needed while providing personal information to the third party through its website, as well as answering individual concerns received via Inquiry Line for Act on Protection of Personal Information.

In the interest of preventing further spread of COVID-19, some efforts are being made to early detect the symptoms of COVID-19 including taking temperature of individuals at various locations in Japan. There are many business operators requiring their

employees to take their temperature daily and some use this as an indicator whether to allow the employee to come to the office or work from home.

The PPC's Inquiry Line for Act on Protection of Personal Information receives many calls on how to properly handle this information (temperature of an individual), and the PPC Japan responds to these inquiries by introducing the relevant articles of the Act on Protection of Personal Information etc.

Jersey - Jersey Office of the Information Commissioner (JOIC)

1. Contact tracing and location tracking

Jersey has not yet adopted a technical solution for track and trace. However, it is looking to develop a privacy-friendly App similar to that of Ireland. Work is underway between the government of Jersey and Digital Jersey (a local organisation that seeks to attract digital businesses to Jersey) to develop the App.

The Government of Jersey currently has a manual track and trace programme, whereby anyone who tests positive for COVID-19 through the testing on arrival at any of Jersey's ports, or anyone testing positive through workplace testing provides details of anyone they have been on contact with, or details of where they were seated on the aircraft or ferry. The Government of Jersey has a robust track and trace team which has been effective in identifying those in close proximity to people testing positive for COVID-19.

Similarly, all organisations allowing patrons to enter their premises (whether retail or hospitality) are required by the Government of Jersey to ask their patrons to provide contact details (name, telephone number and/or email address) for track and trace purposes. Where somebody tests positive for COVID-19, the relevant details of other patrons will be shared with the Government of Jersey through the gateway of 'legitimate interests' under the Data Protection (Jersey) Law 2018.

For licensed premises, those organisations are required to seek contact details from any patrons in accordance with their license conditions issued subsequent to the Licensing (Jersey) law 1974, and under the power of a 1934 Public Health law, which allows the Minister to make such requirements as are deemed necessary in circumstances such as a global pandemic. Those licensed premises must ask for the contact details of patrons. However, patrons are not obliged to provide the details and cannot be refused entry if they refuse to provide them.

The JOIC has published much guidance in relation to a number of areas surrounding the implications of COVID-19. For example:

- Contact tracing checklist;
- Return to work – Privacy considerations;

- Measures relating to transparency;
- Guidance to volunteers;
- Frequently asked questions;
- Healthcare;
- Human resources and employment;
- Working from home: Practical tips for keeping client, staff and volunteer information safe;
- Advice to the general public; and
- Tips for individuals and businesses on video conferencing.

All guidance relating to the Coronavirus outbreak can be found at the dedicated website hub:
https://jerseyoic.org/resource-room/dp-covid-19-contact-tracing/?audience=everything

2. Sharing of health data with health authorities and institutions

Where somebody tests positive for COVID-19, the relevant details of other patrons will be shared with the Government of Jersey through the gateway of 'legitimate interests' under the Data Protection (Jersey) Law 2018.

The JOIC maintains a position of independence and oversight to ensure the Government of Jersey and local organisations remain compliant with the provisions of the Data Protection (Jersey) Law 2018.

Regarding retention of health data, the understanding of JOIC is that contact tracing information will only be retained by the organisation collecting the data for a period of 21 days before being deleted. Similarly, once shared with the Government of Jersey, data used by the Government for tracking and tracing purposes have also been committed to deletion after 21 days. Any publication of the contact tracing data findings is fully anonymised.

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in Jersey on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

Not applicable.

The JOIC has published guidance for charitable organisations and NPOs.

5. Handling of employee data in work-from-home / return-to-work situations

The JOIC has not received any complaints related to the handling of employee data in work-from-home / return-to-work situations. However, the JOIC has dealt with a number of general enquiries relating to COVID issues, for which advice and guidance has been given.

The JOIC has published specific guidance in relation to work-from-home/return-to-work situations. This guidance covers the following areas:

- Internet, Wi-Fi and manual data security;
- Working from home policies and procedures;
- Data breach risks;
- Data collection and storage;
- Retention of data;
- Data sharing;
- Privacy of staff members diagnosed with COVID-19; and
- Return of work-from-home devices.

Please see the guidance suite published by the JOIC at https://jerseyoic.org/resource-room/dp-covid-19-contact-tracing/?audience=everything.

Liechtenstein - Data Protection Authority

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

1. Contact tracing and location tracking

Liechtenstein has not adopted any of its own official digital contact tracing or location tracking measures so far. However, the health ministry recommends on a voluntary basis the use of the Swiss proximity tracing solution (mobile app) based on DP-3T protocol and using Bluetooth technology (SwissCovid App).

Furthermore, in case of a confirmed Covid-19 infection, the health ministry conducts a manual contact tracing based on the information provided by the infected person. The SwissCovid App was developed in Switzerland and therefore is primarily under the scrutiny of the Swiss data protection authority (EDÖB). The DPA Liechtenstein has not been involved in its development or testing.

For details of the Swiss contact tracing application (SwissCovid App), please consult information given by the Swiss data protection authority (EDÖB):
https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#964113395

And general information given by the Swiss Federal Office of Public Health:
https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html

Detailed documentation is also available on github:
https://github.com/DP-3T/dp3t-sdk-backend/security/advisories/GHSA-5m5q-3qw2-3xf3

However, the DPA Liechtenstein was engaged in an open and constructive dialogue with the developers of two other digital contact tracing applications. Based on this, the DPA Liechtenstein gave accordingly recommendations to the health ministry, who had to approve the applications. However, up until today neither of the applications has received approval or a recommendation by the health ministry.

For the two not approved Liechtenstein applications the DPA Liechtenstein required them to implement strongest measures regarding a privacy by design approach, in order to fulfil GDPR requirements and secure proportionality of the contact tracing measures.

When evaluating the additional contact tracing applications, the DPA Liechtenstein applied the restrictive regulations by the GDPR as well as by the Liechtenstein data protection and telecommunications law, targeted at reducing the risks for the rights and freedoms of natural persons as far as possible and constantly securing proportionality of the necessary data processing (encompassing all of the points mentioned above, like privacy impact assessment, data minimization etc.).

2. Sharing of health data with health authorities and institutions

Positive infections with Covid-19 have to be notified notably by medical institutions (and some others) with the health ministry, including data to identify the infected person or persons likely to be infected, in order to detect, monitor and fight the spread of an epidemic. This is regulated by law.

Data can be retained for a maximum of ten years, except if their processing is necessary for a longer time due to the characteristics of a certain disease. Thereafter they will be destroyed or anonymized.

The general good practices promoted by the DPA Liechtenstein for data processing derive from the GDPR and data protection law in Liechtenstein. They encompass things like data minimization, lawfulness of processing, proportionality of processing, transparency, data retention limitations, data subject rights, etc.

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in Liechtenstein on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Liechtenstein on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The DPA Liechtenstein have not come across any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

The major privacy issue identified in relation to handling employee data in work-from-home/return-to-work situations concerns data security.

The following good practices are promoted:

- Using only technical infrastructure provided by the employer;
- Not sharing any information with unauthorized persons;
- Making phone/video calls in closed rooms only without unauthorized listeners;
- Locking of technical devices when not in use;
- No disposal of paper or data storages containing personal data in regular waist bins etc.;
- Turning off microphones and cameras when not in use; and
- Immediate notification of (possible) data breaches with the employer, etc.

Luxembourg - Commission Nationale pour la protection des données (CNPD)

1. Contact tracing and location tracking

Up to date, there is no digital tracing in Luxembourg, but only manual contact tracing (analog tracing).

Information on Luxembourg testing strategy can be found here https://coronavirus.gouvernement.lu/en.html.

The CNPD has been consulted by the Luxembourg governmental Covid-19 task force. The CNPD gave its opinion about the risks from a personal data protection perspective relating to the idea of digital tracing. As for the moment, the government doesn't want to implement a tracing app, and the CNPD has not yet taken further measures. The authority has recommended conducting a data privacy impact assessment, to respect the GDPR's principles, as minimisation, privacy by default and by design, transparency and limitation of data retention, notably. It recommends following the EDPB papers on the matter.

2. Sharing of health data with health authorities and institutions

The manual contact tracing is exclusively carried out by the National Direction of health of the Ministry of Health in accordance with the modified law of 17 July 2020 on measures to fight the Covid-19 pandemic (**the Law**) notably.

Article 10 of the Law provides that "In order to monitor the spread of the SARS-CoV-2 virus, the Health Director is setting up an information system containing personal data."

The personal data processed are made anonymous three after their collection (Article 10 (5) of the Law).

Under certain conditions, data may be processed for scientific, historical research or statistical purposes if pseudonymised within the meaning of Article 4(5) of the GDPR (Article 10 (6) of the Law).

3. Sharing of health data with law enforcement agencies

To the CNPD's knowledge, there is no requirement, arrangement or plan in Luxembourg on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

The CNPD is unaware of any requirement, arrangement or plan in its jurisdiction on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The major privacy issues identified in organisations in relation to handling of employee data in work-from-home / return-to-work situations are the treatment of unappropriated personal data and health data in particular, without legitimate purpose and/or legal basis and without delivering clear information to the employees. The CNPD recommends that private and public entities may only process the personal data which are strictly necessary for compliance with their legal obligations, meaning necessary to implement organisational measures (e.g. remote working, exemption from work, referral to a doctor or the Health Inspection), training and information measures, as well as measures to prevent professional risks.

However, public and private entities cannot compile files containing the body temperature of their employees or agents or diseases (the "comorbidities") which may be aggravating factors in the event of a COVID-19 infection. Furthermore, it is not their role to carry out investigations or "contact tracing". This task falls to the National Direction of health of the Ministry of Health from the moment an employee or agent is tested positive for COVID-19.

For more details about the CNPD's recommendations on collection of personnel data in the context of a pandemic crisis can be found on:
https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html.

For more general guidance: https://coronavirus.gouvernement.lu/en.html.

The CNPD received and is dealing with some information request from controllers or data subjects and some complaints relating to the handling of employee data in work-from-home / return-to-work situations.

Netherlands - Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

AUTORITEIT
PERSOONSGEGEVENS

1. Contact tracing and location tracking

The contact tracing app

- Our national government is still in the process of rolling out a national contact tracing app (CoronaMelder). It is currently being used in parts of the country as a pilot and it is expected to be rolled out nationally in September.
- The app uses the Google/Apple Exposure Notification (GAEN) Framework which is based on Bluetooth Low Energy.
- The app is intended to supplement manual contact tracing, not replace it.
- The app will be voluntary.
- The app and the back-end are open source.
- The app does not store the calculated infection risks and hence cannot be used as a "Covid status passport" of sorts.
- The Ministry responsible for the app and contact tracing has communicated that they will not participate in Phase II of the Google/Apple platform and will continue to roll out its own app, rather than make use of the configuration files etc. from Google and Apple.
- In the pilot the app uses consent as a legal ground for processing, but this is temporary, until a law has been adopted, which is currently under discussion in Parliament which would change the legal basis for processing to Art. 6(1)(e) GDPR. The voluntary nature of downloading/sharing the Temporary Exposure Keys (TEKs) or uploading the TEKs after a positive result will remain after this law has entered into force. To stress the voluntary nature the law will also introduce a provision explicitly prohibiting using any type of (in)direct pressure to use the app.

Privacy by design practices

Firstly, regarding the Google/Apple Exposure Notification Platform. In the basis the GAEN framework is the result of a Data Protection by Design approach., However-

- GAEN is loosely based on DP3T but has not included some of their suggested privacy enhancements; [26]
- GAEN is not under any form of democratic governance;
- GAEN embraces a "don't trust the app" view on privacy and security which collides with the situation in the Netherlands(/Europe) where the app is the result of a democratic process and is open sourced; and
- (As a consequence) GAEN encompasses the calculation of the exposure risk score and it is unclear if this personal health data is shared with servers of Google and/or Apple as part of telemetry practices. [27]

Secondly, regarding the app. Within the limits set by the GAEN framework outlined above, the app has deployed extensive Data Protection by Design measures like:

- removing the IP address of the app user in the hosting environment so it is not processed by the backend server;
- sending bogus queries to the server so network traffic analysis does not convey a possible exposure; and
- not storing the possible exposure status so the app cannot be used as a "Covid Passport".

A DPIA of the app was part of the process. No formal agreements were made with Google and or Apple, and of those parties a DPIA was not received nor has been made available.

The DPIA of the app mentions that tests (code reviews, penetration tests) are an ongoing part of the deployment. As Supervisory Authority the Dutch DPA has not received any reports regarding the outcomes of those, nor have they been made available to the public.

Legislation that forbids data or app misuse is currently being discussed in Parliament. It addresses:

- any form of pressure to use the app and restricts the possibility to use it for any other means than tracing COVID-19. In particular, it explicitly prohibits any form of pressure to use the app of share information from the app with anyone other than the public health authority for the purpose of tracing (possible) COVID-19 infections.
- The most recent version (d.d. 9 September 2020), which has been adopted by our *Tweede Kamer* and will now go on to the *Eerste Kamer* ('roughly' our Senate), has

[26] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf
[27] https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf

the following provision regarding misuse of the app: (unofficial translation)[28]:

Paragraph 8: It is prohibited to compel the use of the notification application or any other comparable digital application or medium. This prohibition shall in any case include the use of the application or medium, the sharing of information thereof, or the communication of whether or not notifications have been received, as a condition for access to a building or facility, the exercise of labour/work, the use of a service, the participation in any form of interpersonal contact, or obtaining any benefit.

- Breach of this prohibition may result in a fine of €8,700- or imprisonment of up to 6 months (such is stated in the law currently discussed by Parliament).
- There is also a specific provision prohibiting the linking of IP addresses shared by the app (when the user of the app with a positive test shares their TEKs with the back-end) so as to prevent identification of the individual.
- The personal data used for the notification application shall only be saved for as long as necessary to notify the relevant data subjects and afterwards will be deleted immediately (such is stated in the law currently discussed by Parliament).

The version of the proposed law is here .

Engagement with the DPA

In the weekend of 18 and 19 April the Ministry of Health, Welfare and Sport held a an 'appathon', a digital event to test and improve new coronavirus apps. 7 Dutch, EU and non-EU apps were chosen from the applications and documentation regarding these apps was shared with the Dutch DPA for assessment. After the weekend the Dutch DPA concluded it had insufficient material to provide a (thorough) assessment of the compliance with the GPDR requirements for (potential) processing of personal (health) data. Especially, it was unclear who would be the controller, what the specific purpose of the app was, and which legal basis would be used for the processing. Afterwards, the Ministry abandoned the idea of using any of the apps from the appathon and decided to create its own app. During this this time the Google and Apple initiative was also launched.

[28] In Dutch : "8. Het is verboden een ander te verplichten tot het gebruik van de notificatieapplicatie dan wel enig ander vergelijkbaar digitaal middel. Onder dit verbod valt in ieder geval het gebruik van de applicatie of het middel, het delen van informatie daarvan, of het meedelen van het al dan niet hebben ontvangen van notificaties daarvan, als voorwaarde te stellen voor de toegang tot een gebouw of voorziening, het uitoefenen van arbeid, het gebruik maken van een dienst, de deelname aan enige vorm van intermenselijk contact, of het verkrijgen van enig voordeel."

This new app was then subjected to a Prior Consultation in the meaning of art. 36 GDPR, before rolling out the application and therefore the Dutch DPA was consulted as the national supervisory authority. Prior to this procedure the Dutch DPA was also in regular contact with the developers of the application.

In the advice following the prior consultation on the 17th of August the Dutch DPA advised that the health minister should make agreements with Google and Apple about the app's software, that legislation should be put in place to properly regulate the use of the app, and that it should be made clear that the app's servers are secure. The Dutch DPA advised the government not to roll out the app until these steps have been taken. See the full press statement here:
https://autoriteitpersoonsgegevens.nl/en/news/dpa-privacy-coronavirus-app-users-not-yet-sufficiently-guaranteed

The Dutch DPA was – in line with article 36(4) GDPR – consulted regarding the draft text of legislation introducing the notification application on 28 May 2020. The Dutch DPA shared our views on the legislation on 8 June 2020. The final text can be found here (DUTCH). The final version differed substantially from the one the Dutch DPA consulted on.

National legislation is currently being discussed in parliament. The server setup has been addressed. No further agreements with Apple and Google have been made so far. The Government has stated that accepting the Terms & Conditions of the app and a further clarification by Apple regarding their processing of personal data is sufficient. A motion by two Members of Parliament regarding the need for control on the Google & Apple framework by the Government, i.e. that the Dutch government can decide when the framework should be 'switched off', rather than Google & Apple is currently still awaiting a response from the Government.

No additional role besides the general supervisory role as the national supervisory authority has been conferred.

2. Sharing of health data with health authorities and institutions

There is a chain of health institutions with different responsibilities.

A general practitioner (GP) is required to report suspicion or diagnoses of an infectious disease on the basis of article 22 of the Law of Public Health (Wet Publieke Gezondheid, WPG) to the Municipal Health Services (Gemeentelijke Gezondheidsdiensten (GGDs)).

The doctor has to provide the following information:

- the name, address, sex, date of birth, citizen service number and place of residence of the person concerned;
- the infectious disease or a description of the clinical picture, the first day of illness, the vaccination status, the use of chemoprophylaxis, the suspected source of infection, the date of suspicion or detection of infection, the method of detection of that infectious disease; and
- if necessary, whether the person concerned or a person close to him or her is professionally or commercially involved in the treatment of food or drink or in the treatment, nursing or care of other persons.

However, currently tests for COVID-19 are performed by special testing facilities set up by the Municipal Health Authorities. If someone suspects they have COVID-19, they are referred to these testing facilities, rather than to their GP. So it will not be that common (anymore) that this information chain starts with the GP, but rather at the testing facility.

The Public Health Act provides for the processing of personal data by Municipal Health Services (Gemeentelijke Gezondheidsdiensten (GGDs)) for the purpose of source and contact tracing. In doing so, they keep a database pursuant to Section 29 of the Law of Public Health (Wet Publieke Gezondheid, WPG). As stated, the GGDs are responsible for the free testing available to all people.

The GGDs must then report this to the RIVM (Rijksinstituut voor Volksgezondheid en Milieu, our National Institute of Public Health and the Environment) and state the details referred to in Article 28 of the WPG.

These details are:

- the infectious disease or a description of the clinical picture, the first day of illness, the vaccination status, the use of chemoprophylaxis, any hospitalisation, the suspected source of infection, including, if necessary, the resulting cases, the date of suspicion or detection of infection; and
- the sex, month and year of birth of the person concerned and the first three digits of the postal code of his/her address, and in case of death – the location of the body.

Regarding health data retention, it is determined in art. 28 of the WPG that the Municipal Health authorities cannot keep the data longer than 5 years. The RIVM does not have any information on retention periods for the data they have.

3. Sharing of health data with law enforcement agencies

The Dutch DPA are unaware of any requirement, arrangement or plan in your jurisdiction on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in the Netherlands on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic

5. Handling of employee data in work-from-home / return-to-work situations

The fact that many people work from home due to the Corona crisis may mean that the security is less organized than at the office. This might make data breaches more likely. Furthermore, organisations might be more likely to become victims of cybercrimes. Hence, the Dutch DPA has drawn up some tips regarding working from home.

Tips on good privacy practices were drawn up regarding the following subjects:

- Work in a secured (online) environment
- Secure sensitive documents
- Be mindful of what video-conference application you use
- Beware of phishing emails

Also some FAQ's regarding working from home were published on the website of the Dutch DPA (only available in Dutch):

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/veilig-thuiswerken-tijdens-corona
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/corona-op-de-werkvloer
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/temperaturen-en-gezondheidscheck

New Zealand - Office of the Privacy Commissioner (NZ OPC)

1. Contact tracing and location tracking

Contact Tracing Measures

The primary contact tracing mechanism at the time of writing is the NZ COVID Tracer App (developed by the Ministry of Health). Other options are still being pursued (e.g. Bluetooth exposure notification framework, Bluetooth proximity hardware ('CovidCard').

Various private sector Apps have also been developed for individuals or agencies to record where individuals have visited. In May 2020 the NZ OPC provided a summary of many of these Apps at *https://privacy.org.nz/blog/assessing-contact-tracing-solutions/* .

Note that the remainder of our survey response relates to government initiatives, unless otherwise stated.

The COVID Tracer app allows individuals to scan QR codes at locations, including public transport, workplaces, businesses, public places. There is also functionality to record manual entries (e.g. free text fields to record location). This acts as a digital diary, which is used by individuals to record their movements. The digital diary can be provided to Ministry of Health contact tracers (by consent of the individual concerned) to assist with contact tracing. Additionally, contact alerts can be sent notifying individuals of a possible exposure to someone with COVID-19. The Ministry of Health can send an alert to all app users for specific QR location(s). Phones will then run matches in the background to see if the user has scanned into the location at a given time – similar to the Exposure Notification framework matching but with QR codes instead of unique codes.

Bluetooth technology is still being considered by the Government.

The existing digital measures and any future additions will only be supplementary to traditional contact tracing. Manual contact tracers by trained staff is still very important. Digital contact tracing can help with speed of identifying contacts, provision of contact details, and identifying unknown contacts.

The kinds of data collected by the COVID Tracer app and by manual contact tracing includes the following:

COVID Tracer app:

- name, contact details (email address, address, etc)
- scanned QR locations (stored locally on device until requested by a contact tracer and provided to contact tracer by consent)
- telemetry about the phone for analytics (de-identified information)
- National Health Index (NHI) number (stored on phone, used to help individuals who need to get COVID tests, as NHI numbers are used in testing process)

Manual contact tracing:

- Name, contact details
- Close contacts, contacts: contact and other information required about those contacts
- Locations visited
- The circumstances in which he or she believes he or she contracted or transmitted COVID-19

The information is used by contact tracers when interviewing positive cases to identify potential transmission of COVID-19, including where a positive case was infected with COVID-19 and who they may have subsequently infected.

The scanned QR locations operate both as a trigger for memory for individuals and contact tracers during the conversation, and also to be used as 'contact alerts' to advise individuals that they may have been exposed to COVID-19. This is a secondary usage and has not been used many times in NZ.

Contact data within the app is used to contact close contacts or contacts of those who have tested positive. The rest of the data is used in manual contact tracing as described above, telemetry information is used to de-bug the app.

The data is not ordinarily disclosed to anyone outside of the Health system. In rare events of noncompliance it may be disclosed to Police to enforce compliance with requirements under the Health Act.

App usage and provision of information is entirely voluntary. Individuals have a duty under section 92ZZC of the Health Act to provide information about their contacts to contact tracers, but this does not mandate the use of the app. Individuals are also required to either scan a QR code or provide contact details when entering certain businesses, under Ministerial Order.

Engagement with the NZ OPC

For NZ COVID Tracer the Ministry of Health extensively engaged the NZ OPC. It was an iterative process of engagement with the design and privacy impact assessment. A thorough privacy impact assessment was undertaken and was revised with subsequent iterations of the app.

The NZ OPC has relied on its existing role which includes advising on privacy matters affecting New Zealanders.

The NZ OPC has reviewed the privacy impact assessments, considered design options and monitored overseas developments in the digital contact tracing space. The NZ OPC has assessed international digital contact tracing solutions (link: https://privacy.org.nz/blog/the-app-race-to-contact-trace/) and evaluated domestic contact tracing options (link: https://privacy.org.nz/assets/2020.06.12-Contact-tracing-solutions-table.pdf). The NZ OPC has also provided guidance and blog posts about contact tracing and encouraged agencies not to use contact tracing information for any other purpose: https://privacy.org.nz/resources-2/privacy-and-covid-19/information-about-contact-tracing/.

Privacy by design practices

A privacy by design approach was taken to develop the COVID Tracer app. It doesn't collect more information than is necessary and informed consent is integral to using the app. It doesn't automatically share data without consent of the individual.

The app developers utilized all of Government security experts, independent audits and testing, and leveraged existing technology which had been thoroughly tested and audited for security. There are no specific privacy protections for the app enshrined in legislation.

There are no specific notification requirements regarding the improper access to the data in the app, but under the Privacy Act 2020 (in effect 1 December) agencies will be required to notify the OPC (and affected individuals) of privacy breaches that cause or may cause serious harm. The Privacy Act does not include a civil penalties regime that applies to the improper use and access to the data. The OPC would investigate a complaint of improper use or access to the data. There will be no mandatory review of the digital measure, but statistics on usage are provide by the Ministry of Health frequently.

The information collected by the app will be held for the duration of the pandemic or until no longer required. There is no set timeframe on when the app will be rolled back/discontinued. The QR scans which stay locally on devices are only stored on the device for 60 days.

2. Sharing of health data with health authorities and institutions

The health sector is devolved in New Zealand and data is shared between the different health agencies that form the health sector. The NZ OPC was not involved in the development of the policy that the Ministry of Health developed.

The NZ OPC is not aware of plans to retain data for the purpose of specific research, but New Zealand has the Health (Retention of Health Information) Regulations 1996 which overrides the Privacy Act and requires health records be kept for a minimum of 10 years after the date that an individual ceased treatment/healthcare. Rule 11 of the Health Information Privacy Code allows for health information to be disclosed for research purposes on with approval by an ethics committee (if required), and the health information will not be published in a form that could reasonably be expected to identify the individual concerned.

Following public concerns about the distribution of COVID-19 patient details across the Health sector due to a privacy breach incident, the OPC has initiated an own-motion Inquiry into the arrangement: *https://privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-inquiry-into-distribution-of-covid-19-patient-information/*

The OPC provides a range of privacy advice to health authority and institutions (including the website and also responses to specific questions). The forthcoming Inquiry report relating to the sharing of COVID-19 patient details is also relevant.

3. Sharing of health data with law enforcement agencies

The Ministry of Health had shared health data (e.g. identifying infected individuals) with New Zealand Police in relation to vetting individuals.

This information sharing has ceased. When the OPC became aware of the information sharing with New Zealand Police, it raised concerns with Police and Health and this information flow stopped. This line of concern became part of the inquiry into the distribution of COVID-19 patient information. The Privacy Commissioner has been clear that COVID-19 information should not be used for Police vetting purposes.

4. Sharing of health data with charitable or other similar organisations

Data may be being shared with charitable organisations under the Privacy Act (or otherwise) but the OPC is not aware of any specific arrangements on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

Major privacy issues identified in the handling of employee data in work-from-home/return-to-work situations include:

- Security of technology solutions to enable working from home
- Monitoring of employees (e.g. webcams/audio to check that employees are working)
- Security of information when stored at home
- Contact tracing in the workplace when returning to work

The OPC encourages privacy impact assessments to be completed prior to the implementation of new technologies.

The OPC also provided advice about working from home (https://privacy.org.nz/further-resources/knowledge-base/view/561?t=233661_321552) and contact tracing in the workplace (https://privacy.org.nz/further-resources/knowledge-base/view/565?t=233661_321552).

The OPC has received enquiries from individuals who held concerns about their employers' privacy practices in respect of working from home. The OPC asked for more information and provided guidance to the affected employees.

Philippines - National Privacy Commission (NPC)

1. Contact tracing and location tracking

Digital measures are intended to supplement manual contact tracing.

Digital measures 1: StaySafe.ph

- Developer: Multisys Technologies Corporation
- StaySafe.ph is a cloud-based, community-driven Contact Tracing, Social Distancing and Health Condition Reporting System. It was designed and developed by MultiSys, in partnership with PLDT-Smart Group and PLDT Enterprise, to respond to the novel coronavirus disease (COVID-19) pandemic outbreak. With StaySafe.ph, site visitors can contribute to the fight against COVID-19 by reporting their own health conditions.
    - StaySafe.ph uses digital tools to help protect individuals in response to the pandemic. Site visitors also have an option to help through service (for frontliners, doctors and health workers) and suggestions.
    - This will help the private sector and local government units attend to immediate assistance needed by employees or locals under their jurisdiction—making it easier to track COVID-19 on a national basis.
    - StaySafe.ph uses GPS location primarily for detecting and monitoring the data subjects' health conditions and general location. It aggregates maps of those areas according to overall condition and responds to data subjects needing assistance from the Department of Health.

The clinical data are stored solely in the Department of Health's filing system. The Department of Health provides an Application Programming Interface (API) to inform StaySafe.PH on a case (either a yes or a no). The data will be usually disclosed to the Department of Health and other relevant government agencies to monitor the COVID-19 cases and health conditions of the populace.

Digital measure 2: TraceFast

TraceFast is a separate app developed by Multisys Technologies Corporation that uses the Google-Apple Exposure Notification (GAEN) API which works through the secure exchange of keys via Bluetooth technology.
The usage of the app is voluntary. Data subjects can uninstall the app and manually request for their data to be deleted.

In general, the digital and manual contact tracing measure collect the following kinds of data:

- Health Status
- Mobile Number
- Symptoms
- Geo-Location
- For QR CODE (Digital Logbook Feature)
- Name
- Age
- Gender
- Residence
- Company Name
- Company Address
- Photo

Privacy protection of the apps

In terms of the privacy protection aspect of the apps, the proponents of the digital measures are cooperative. They have open and constructive engagements with the National Privacy Commission. The National Privacy Commission was consulted on data privacy matters especially with the implementation of contact tracing and the location tracking through GPS. Multiple iterations of Privacy Impact Assessments are undertaken by the proponents of the digital measure, considering the comments of the privacy authority.

The developers addressed matters of data security and safeguards employed to protect data collected by the digital measure by:

- Unauthorized disclosure - To reduce this risk, admin personnel will only have limited access based on their assigned roles and scope of work.
- Potential misuse of data by authorized users - To reduce this risk, they will implement reasonable and appropriate physical, technical, and organizational measures to prevent data loss and destruction.

- Denial of Service – To reduce this risk, network security will be checked regularly.
- The Data Privacy Act of 2012 has privacy protections in place and addresses these potential data privacy violations

The retention period is currently being finalized, specifically by the Department of Health. As discussed during the recent meeting, the Department of Health is considering a 30 or a 60-day retention period.

An incident response plan was also created regarding the improper access to the data. The Department of Health, as the controller, also performs the monitoring and evaluation of its projects, including the StaySafe.PH app. Please refer to the Telemedicine Regulatory Sandbox – for the Joint Memorandum Circular with the National Privacy Commission, see the Guidelines on the Use of Telemedicine in COVID-19 Response which is available at https://www.privacy.gov.ph/wp-content/uploads/2020/05/DOH-mc2020-0016.pdf.

In the case of improper use and access to the data, accountability penalties may apply: https://www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/#51 .

The NPC would also promote good practices such as collecting only what is necessary, and disclosing only to the proper authorities, on the use of contact tracing or location tracking measures. The NPC published 'Guidelines on the Use of Telemedicine in COVID-19 Response', available at https://www.privacy.gov.ph/wp-content/uploads/2020/05/DOH-mc2020-0016.pdf.

2. Sharing of health data with health authorities and institutions

Sharing of health data with health authorities and institutions is governed generally by the Data Privacy Act. This is supplemented by special laws covering contact tracing effort such as Republic Act 11332 otherwise known as Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act, which requires the Philippine Department of Health and local governments to implement protocols for reporting and response, including contact tracing activities, to contain highly infectious diseases like COVID-19.

Data may be retained as long as necessary to achieve contact tracing efforts, depending on issuances and directives of public health authorities.

Under the Data Privacy Act, data sharing agreements covering health information among and between government agencies is within the purview of the NPC, including the review and assessment of such agreements to determine whether it confirms to the general principles of privacy, and the provisions of the DPA. The NPC also issued NPC Circular No. 16-02 which governs data sharing agreements between government agencies.

In addition to the foregoing, the NPC works in close coordination with the Philippine authority, the Department of Health, to ensure that only necessary data is collected by health institutions, and that such data is disclosed only to proper authorities. The NPC has issued joint statements to this effect (See NPC PHE Bulletin Nos. 3, 7, 11 and other related issuances).

To date, the Department of Health (DOH) has issued circulars covering the anonymization and protection of data, especially relating to health information of COVID-19 patients. This was a result of NPC's close coordination with DOH. For example, DOH has issued 2020-002 which establishes Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response.

3. Sharing of health data with law enforcement agencies

The mechanism of sharing of health data with law enforcement agencies is covered by the Inter-Agency Task Force on Emerging Infectious Diseases (IATF) which is organized to assess, control, monitor, contain and prevent the spread of the COVID-19 pandemic. The Task Force is authorized to share data among government agencies, including law enforcement, to attain their mandate.

The NPC has provided the IATF with guidelines, opinions, and reminders so that government interventions will consider privacy for all interventions that require the processing of data. Likewise, NPC has NPC Circular No. 16-02 which provides guidelines for Data Sharing Agreements involving government agencies.

Under NPC Circular No. 16-02, the NPC offers review of Data Sharing Agreements to promote its use, and to support law enforcement agencies formulate and craft DSAs. This additional intervention by NPC ensures that DSAs will be in conformity with the Data Privacy Act and other issuances of NPC.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in the Philippines on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

Privacy issues faced by both the government and the public sector in work-from-home arrangement are associated with security vulnerabilities in unprotected personal devices and home networks which do not have the same level of protection as compared to the workplace.

NPC issued Bulletins which lay down guidelines to safeguard personal data in work-from-home arrangements (See NPC PHE Bulletin No. 12) as well as frequently asked questions that employers and employees can refer to in formulating their policies as they return to work (See NPC PHE Bulletin No. 14).

To date, NPC has not received complaints, breaches or investigations related to work-from-home / return-to-work arrangements. Nevertheless, the Complaints and Investigation Division are ready to receive complaints and act on these matters as may be necessary.

Poland - Personal Data Protection Office (UODO)

1. Contact tracing and location tracking

Contact tracing apps and measures

Due to COVID-19 pandemic, the Ministry of Digital Affairs introduced two applications aiming at counteracting the coronavirus crisis:

I. Home Quarantine – ("*Kwarantanna Domowa*") 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.

In order to properly and fully use the Application, the User should have a mobile device with the Android 6.0 or higher system with access to the Google Play or iOS store, version not lower than 10.3 and with access to the AppStore, a GPS module and with access to the Internet and equipped with a camera with a minimum resolution of 5Mpix and the possibility of video recording.

The periodic quarantine verification service consists of the following steps:

- confirmation of being in the declared location. When performing this task, the GPS location is automatically checked,
- taking a "selfie" photo at the declared location.

Other language versions (e.g. Russian and Ukrainian) have been also added to the application.

According to the its regulations, the ‘Home Quarantine’ app gathers data such as: Citizen's technical identifier, Full name, telephone number, Declared residence address, Photograph of the person, Citizen's location (declared quarantine location and location designated by the system during the verification task), Quarantine End Date.

More information in Polish is available on the government website: https://www.gov.pl/web/koronawirus/kwarantanna-domowa

II. Protego Safe – 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 people 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.

ProteGO Safe 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.

The installation and use of the ProteGO Safe application takes place on a voluntary basis.

In the ProteGO Safe 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 ProteGO Safe 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."

ProteGO Safe application does not require to give any personal data at any stage of use of the application. ProteGO Safe does not collect personal data either. All the information processed by ProteGO Safe are processed in a way making the identification of users completely impossible.

Information on ProteGO Safe application is available in Polish on the government website: https://www.gov.pl/web/protegosafe/jak-to-dziala/

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

In addition, the Ministry of Digital Affairs has developed a system that collects anonymous data from mobile network operators to monitor how phone users move. It is a system that allows for the development of, e.g. analyses of the movement of users - more precisely their phones, between different regions of the country, including anonymous data from telecommunications operators. This system allows to see the mobility of residents between specific poviats.

Engagement with the UODO

The Ministry of Digital Affairs has consulted the Personal Data Protection Office on the ProteGO Safe application and its general functions.

According to the government statements, "the ProteGO Safe application is built in accordance with the principles arising from the General Data Protection Regulation (GDPR), including data minimization, privacy by design, privacy by default, accuracy, integrity and confidentiality. Moreover, the government declares that the application is based on the guidelines of the European Council for the Protection of Personal Data, the European Commission and Toolbox developed as part of the eHealth network operated by the European Commission".

As regards ProteGO Safe application, the Personal Data Protection Office was only indirectly involved. Due to the state of epidemic no inspections in this regard have been conducted so far. 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.

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 has issued a recommendation regarding the general use of applications: https://uodo.gov.pl/en/553/1143.

2. Sharing of health data with health authorities and institutions

NIL.

3. Sharing of health data with law enforcement agencies

NIL.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Poland on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

To date, the Personal Data Protection Office does not conduct any case related to the handling of employee data in work-from-home / return-to-work situations. Neither has the Office issued any decision on this matter.

The Polish SA developed guidance on "Security of personal data during remote learning" (https://uodo.gov.pl/en/553/1118):

For a principal-

- It is the obligation of the school to inform teachers, parents and students about the methods of conducting distance education. This information should be

provided in a clear manner so that it is understandable for everyone who is targeted by this announcement. If the school, in order to provide distance education, would use new tools or services offered by external entities, it is obliged to inform on the scope of personal data being processed.

- The school should provide the tools enabling the teachers to conduct classes remotely and to safely communicate with students and their parents – implementing these tools in the unit in a comprehensive manner.
- In the event of carrying out their work-related duties by the teachers outside the school premises, the principal must in any case consider the options that allow adequate data protection level, taking into account the level of risk of data protection breaches, and must implement adequate measures to mitigate this risk, or resign from conducting activities that pose such risks, e.g. allowing the teacher who does not have the conditions necessary to conduct remote work to use the equipment stored in the school premises.
- The principal should not recommend to the teachers the use of their private e-mail addresses for contacting their students or their parents / legal guardians. It is recommended that the teachers use their work e-mails to contact their students. However, in both cases they should be adequately safeguarding the personal data being disclosed in their messages.

For a teacher-

- The teacher must keep in mind to safely use the computers and other devices both when these were provided by the employer, and when using personal equipment.
- If the teacher is using his/ her own device, he/she should independently fulfil the fundamental security requirements. First of all, it is necessary to verify, whether the device being used is equipped with an up-to-date operating system, whether the software is being used, especially antivirus software, and whether the necessary updates were installed. Anti-malware and antispyware software should also be kept up to date. It is necessary to install the software in a cautious manner and it should be downloaded only from reliable sources (the websites of their manufacturers).
- When using the software or mobile applications it is necessary to use all technically possible mechanisms that protect the privacy of the users. If the usage of some of the software requires logging in, it is worthy to care for a strong password, additionally protected from loss and the access by unauthorised persons.
- To a basic extent, communication with students and parents is carried out through ICT solutions implemented by the school, e.g. electronic school registers. In this situation, the teacher must still observe the basic safety rules

while connecting to the electronic school register remotely from his/her device at home.

- Conducting classes remotely may require the teacher to use electronic mail to contact students or parents. The teacher should keep correspondence from the official mailbox, which should be provided by the school. If the school has not provided teachers with official mailboxes, teachers must remember that private mailbox should be used for business purposes in a prudent and secure manner.
- In order to conduct distance learning, the teacher should use educational platforms or e-learning tools that have been implemented at school. In such situation, the teacher can expect that conducting classes remotely will be safe. The teacher should follow the school's instructions and procedures for the personal data protection and must maintain basic security principles when connecting to such a platform remotely from his/her device at home.
- In the current situation, in consultation with the school headmaster, the teacher should take into account what real options the students and parents have for communicating with the teacher, provided that the specific type of internet messenger indicated by them ensures the security of communication.

The Polish Supervisory Authority also developed good practices that help keep data secure during online lessons (https://uodo.gov.pl/en/553/1118), in which 20 security principles should be kept in mind by school controllers as well as teachers and students when preparing for online lessons to protect their data were proposed:

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.

San Marino - San Marino Data Protection Authority

AUTORITA' GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

1. Contact tracing and location tracking

NIL.

2. Sharing of health data with health authorities and institutions

There is no requirement, arrangement or plan in San Marino on sharing of health data with health authorities and institutions for fighting COVID-19.

In the case of (any) data sharing arrangement, it is necessary to ask San Marino DPA for the prior opinion.

The San Marino DPA promotes good practices in relation to data sharing with health authorities and institutions by organising training courses, meetings, awareness-raising campaigns. It provides support to the Public Administration and publish information contents on the website.

Health data will not be retained for research in the public interest at the moment.

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in San Marino on sharing of health data with law enforcement agencies for fighting COVID-19.

In the case of (any) data sharing arrangement, it is necessary to ask the San Marino DPA for the prior opinion.

The San Marino DPA cooperates with the law enforcement agencies where they ask for opinion.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in San Marino on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

In the case of (any) data sharing arrangement, it is necessary to ask us for the prior opinion.

The San Marino DPA is also currently working on the good practices in relation data sharing with charitable or other similar organisations.

Health data will not be retained for research in the public interest at the moment.

5. Handling of employee data in work-from-home / return-to-work situations

The San Marino DPA has not received any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

The major privacy issues in relation to handling of employee data in work-from-home / return-to-work situations are related to the use of technological solutions, platforms and services on the Internet.

The San Marino DPA raises awareness of people about the risks on the use of the Internet but it is a well-known matter unrelated to the COVID19 issues anyway.

The San Marino DPA does not have specifically written good practices in this regard, but it is working on them. However, it provides some suggestions to mitigate privacy issues better.

Slovakia - Office for Personal Data Protection of the Slovak Republic

1. Contact tracing and location tracking

A digital contact tracing app is developed by the developer '**eKaranténa**'. It supplements manual contact tracing.

After arrival to Slovak Republic from countries marked as "dangerous", instead of going to public quarantine place, you can download this application and stay at place of your choice. The fact that you are staying home is ensured by location tracing and face biometric recognition via your smart phone.

The underlying technologies employed include Bluetooth technology; Location tracing; biometric face recognition functionality.

Location data will be collected from the data subjects to check if they are compliant with quarantine regime. The data will usually be disclosed to the police.

Although the use of the app is voluntary, if you did not want to use it, you go to the state quarantine accommodation with strict regime.

Slovak government has enacted special legislative measures and creates legal basis for processing personal data through eKarantena (more personal data are needed to be processed compared to the classical manual contact tracing and quarantine requirements).

The data collected by the app should be deleted after 21 days.

The Office for Personal Data Protection (OPDP) was not consulted on the measures stated above, although the OPDP plays a Supervisory role twice - once in the process and once after the process (when the application will not be needed anymore). An assessment of privacy risks was also not properly conducted in our point of view. The only information the OPDP has is from official statements and this website: https://korona.gov.sk/ekarantena/ .

As for good practices, the OPDP was not consulted properly on this issue, and it was trying to provide the public with its opinion. However, it did not have chance to get in touch with developers of the application.

2. Sharing of health data with health authorities and institutions

The ways of health data sharing with health authorities and institutions for fighting COVID-19 is already governed by national legislative acts.
The OPDP has basic supervisory and advisory competences granted by GDPR/ national law in this regard. The OPDP is trying to get in touch with authorities, mainly with their data protection officers and elaborate privacy policy and processing activities.

3. Sharing of health data with law enforcement agencies

Health data is shared with law enforcement agencies only if a person was in breach of home quarantine. Some consequences enforced by the police could take place. Also, if a person would be in breach of Criminal Code (Criminal Offence: Spreading of Dangerous and Contagious Disease), then the criminal process would also involve processing of health data. However, this applies not only during pandemic, but also in "standard" life.

To promote good practices in relation to data sharing with law enforcement agencies, the OPDP is trying to get in touch with Data Protection Officers, so that they can coordinate the work of their agencies.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in the Slovakia Republic on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

The OPDP has have yet to receive any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations.

The major privacy issues identified organisation in relation to handling of employee data in work-from-home / return-to-work situations relate to handling with personal data in hard copies of files, as well as insufficient resources for buying relevant IT equipment with proper security measures.

The OPDP promotes good practices in this regard such as:

- using notebooks only for employment-related tasks;
- notebooks should have sufficient security measures; and
- when handling with hard copies of files - properly developed system of managing, such as statistics, which employee has the hard copy of file and for how long etc.

Switzerland - Federal Data Protection and Information Commissioner (FDPIC)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

1. Contact tracing and location tracking

Contact tracing measures

For both digital and manual contact tracing, the Federal Office of Public Health (FOPH), the competent cantonal authorities and the public and private institutions entrusted with tasks in accordance with the EpidA process personal health data in accordance with Section 2 of the EpidA, insofar as this is necessary to identify persons who are ill, suspected of being ill, infected or suspected of being infected, with a view to implementing measures to protect public health. In doing so, they shall also observe the general principles of federal and cantonal data protection legislation. Hospitals and other public or private health care institutions, as well as laboratories and medical personnel, are also subject to special reporting obligations under the EpidA.

The cantonal authorities are responsible for tracing chains of transmission. This is what they do. When a person tests positive for the coronavirus, the cantonal authorities work with that person to ascertain who they have been in close contact with – in the 48 hours before the symptoms of the disease developed, up to the point at which they went into isolation. The authorities notify the persons identified that they may be infected.

The SwissCovid app for mobile phones (Android/iPhone) is helping to contain the new coronavirus. It complements the conventional contact tracing carried out by the cantons – and thereby helps to break chains of transmission. The use of the app is voluntary and free of charge.

You have to activate your Bluetooth. When within Bluetooth range, the mobile phone exchanges random IDs (identification code) with other mobile phones that have a compatible app installed. The random IDs are stored on the mobile phone for 14 days before being deleted automatically.

If an app user tests positive for the coronavirus, he/she receives a Covidcode from the cantonal authorities. The code allows him/her to activate the notification function in the app, thereby warning app users that came into close contact with the infected person in the period starting two days before that person first experienced symptoms

of the disease. When the code is entered, the app notifies these other app users automatically. The identity of the person who triggered the notification is not revealed. Notification is triggered if the app user has spent at least 15 minutes at a distance of under 1.5 metres from at least one infected person within a 24-hour period. It is possible for someone to be under 1.5 metres away from several infected individuals for less than 15 minutes within the space of a day. As these encounters may exceed a total of 15 minutes, the Swiss Covid app will notify the app user that there is a risk of infection.

The people who have been notified can then call the infoline number in the app and find out what to do next.

Pursuant to Article 12 of the Ordinance on the Proximity Tracing System for Coronavirus SARS-COV-2 (OPTS), the Federal Office of Public Health provides the Federal Statistical Office (FSO) with statistical data periodically and in fully anonymised form.

Before the SwissCovid app was able to be launched, the Epidemics Act had to be amended. To do this, the Federal Council submitted a bill to Parliament. In its June session, Parliament approved the statutory provisions relating to the app, making only minor changes to the draft legislation. This regulates organisational and operational matters, the processed data and using the app. Parliament approved the amendment to the Act on 19 June 2020.

The SwissCovid app system has been developed on behalf of and in cooperation with the FOPH by the Federal Office for Information Technology, Systems and Telecommunication FOITT, the Federal Institutes of Technology in Zurich (ETH) and Lausanne (EPFL) and the Swiss company Ubique.

For the app see the Ordinance on the Proximity Tracing System for the Sars-CoV-2 coronavirus**.**

Engagement with the FDPIC

The FDPIC was contacted by the EPFL at an early stage and has then set up a Corona Task Force. Several videoconferences took place with the EPFL exploring legal and technical issues.

The FDPIC and his Corona Task Force were involved in the implementation work of the Federal Administration for a "Covid proximity tracing app". The implementation is based on the "DP-3T" model developed by the EPFL, which follows a decentralised

approach, and is independent of the developments within the European "PEPP-PT" project.

The FDPIC has issued a Position statement according to Article 17a FADP re the pilot trial with the Swiss Proximity . In particular, it stated that the application design must be transparent and provide data protection by default. The data-protection-by-default approach of the SPTS is reflected in particular in the following design aspects:

- only the proximity between users is relevant, no location data is collected;
- there is no exchange of identifiers with smartphones that have not installed the mobile app;
- it is not possible to track people or devices based on the changing EphIDs;
- unless a person with a confirmed infection sends notification to the server, no data is uploaded to the server;
- only encounters of two metres or less are recorded and they only generate a message if they have lasted for at least 15 minutes on any day;
- data is only stored for as long as is useful to detect possible infections; and
- the use of the system is limited to the duration of the pandemic.

For more information on the good practices promoted by the FDPIC, see our Position statement according to Article 17a FADP re the pilot trial with the Swiss Proximity .

2. Sharing of health data with health authorities and institutions

Following the declaration of the special situation in accordance with Art. 6 of the Epidemics Act (EpidA) by the Federal Council, the federal, cantonal and communal authorities are continuing to work in conjunction with public health institutions to combat the current coronavirus pandemic.

The Federal Office of Public Health (FOPH), the competent cantonal authorities and the public and private institutions entrusted with tasks in accordance with the EpidA process personal health data in accordance with Section 2 of the EpidA, insofar as this is necessary to identify persons who are ill, suspected of being ill, infected or suspected of being infected, with a view to implementing measures to protect public health. In doing so, they shall also observe the general principles of federal and cantonal data protection legislation. Hospitals and other public or private health care institutions, as well as laboratories and medical personnel, are also subject to special reporting obligations under the EpidA.

3. Sharing of health data with law enforcement agencies

NIL.

4. Sharing of health data with charitable or other similar organisations

There is no requirement, arrangement or plan in Switzerland on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic.

5. Handling of employee data in work-from-home / return-to-work situations

Insofar as private parties, in particular employers, process personal data to combat the pandemic, the processing must be carried out in compliance with the principles set out in Article 4 of the Federal Data Protection Act:

- Health data are particularly worthy of protection and, as a matter of principle, may not be obtained by private parties against the will of the persons concerned.
- Moreover, processing of health data by private parties must be purpose-related and proportionate. This means that they must be necessary and suitable with a view to preventing further infections and must not go beyond what is necessary to achieve this goal.
- Wherever possible, appropriate data on flu symptoms such as fever should be collected and passed on by those affected themselves.
- The collection and further processing of health data by private third parties must be disclosed to the data subjects so that the latter understand the purpose and scope of the processing as well as its content and time frame.

Insofar as private individuals collecting medical data such as body temperature before entering buildings or workplaces for the purpose of preventing infection, the processing of this data is to be limited to the minimum necessary to achieve the purpose in terms of its content and time. The information and self-determination of the persons concerned must be respected when collecting data. In this context, answering extensive questions about the state of health to non-medical persons proves to be inappropriate and disproportionate.

The same applies to personal data processed by private individuals in connection with operational and organizational measures to prevent infection. At the latest when the pandemic threat has ceased to exist, these data must be deleted as a whole.

If the use of digital methods for the collection and analysis of mobility and proximity data is considered, they must prove to be proportionate to the purpose of preventing infection. They are only so if they are epidemiologically justified and suitable to have an effect justifying the intervention in the personal rights of the persons affected in order to contain the pandemic in the its current stage.

Turkey - Personal Data Protection Authority

1. Contact tracing and location tracking

Life Fits Into Home (Hayat Eve Sığar- HES) is the application developed by Turkish Ministry of Health and this application can be downloaded to smart phones and tablets. It is a mobile application developed in order to inform and guide the users about the Covid-19 virus and to minimize the risks related to the pandemic and prevent its spread.

By this application;

- The disease or symptom is followed through the user's general health status declaration and the Ministry of Health contacts when necessary;
- The notifications and warnings are received from the Ministry related with the pandemic;
- The transmission risk is evaluated on the map through the user's location;
- There is a notification feature for those who violate the measures regarding social life;
- The travel tracking code (HES Code) is provided to each passenger which enables contact tracing during and after the travel;
- Risk density in the neighbourhoods is available through the QR codes posted at the entrance of public living spaces such as workplaces; and
- It provides information on the general health status and location of the close individuals such as relatives friends or colleagues who have downloaded the user application and consented to share this information.

Life Fits into Home application is a home product developed by the Ministry of Health with technical cooperation of local and international IT companies. The application mainly benefits from Bluetooth and GPS (Global Positioning System) technologies. The data obtained from the application supports the work of the healthcare professionals who perform contact tracing in the field. The categories of data that will be collected by this app include identity data, contact data, location data, health status and professional status.

Citizens can find out the risk status of their general health status and location of the close individuals such as relatives, friends or colleagues in line with their consents, also the location of places such as hospitals, pharmacies, bus stops, markets and the

density of infection risk in the regions through the map. At the same time, citizens can share whether they have the Covid-19 risk by obtaining the HES Code via “Life Fits Into Home App” during their travels. Passengers can thus travel in a healthy and safe manner.

With the “Safe Area” service offered through the application, business owners can see the risk status of the visitors by posting the QR codes they have created in their workplaces through the app, and also citizens can also benefit from the same information.

During the process of developing the app, some exchanges of views took place between the Ministry of Health which developed the application “Life Fits Into the Home” (HES) and the Personal Data Protection Authority of Turkey.

Personal Data Protection Authority of Turkey has a regulatory and supervisory role. After exhausting the remedy of the request to the data controller, the data subject may lodge a complaint with the Authority. Also the Authority can make examination *ex officio* where it has learnt about alleged infringement.

Personal Data Protection Authority of Turkey prepared a public announcement to enlighten the public within the scope of planning and implementing digital contact tracing and location tracking measures which was published on its official website. Source: https://www.kvkk.gov.tr/Icerik/6729/REGARDING-PROCESSING-OF-LOCATION-DATA-AND-TRACKING-MOBILITY-OF-INDIVIDUALS-TO-COMBAT-COVID-19

According to this public announcement, in cases where location data need to be used by relating to a natural person;

- The provisions of Law do not apply in cases where personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned by law to maintain national defence, national security, public security and order or economic security, pursuant to subparagraph (ç) of Article 28(1) of Law No.6698 (Turkish Personal Data Protection Law).
- From this viewpoint, in order to eliminate the threat in situations where public order and public security are threatened by, such as, an epidemic disease, data processing activities to be carried out by competent public institutions and organizations in order to ensure isolation of people who have been diagnosed with the disease, to identify crowded areas by processing location data of the general population and to develop measures in these areas, are evaluated under the subparagraph (ç) of Article 28(1) of the Law.

- In this context, there is no obstacle to the processing of location data by the competent institutions and organizations which fall under the scope of the mentioned article, in order to prevent the spread of the disease caused by COVID-19 that threatens public security and public order.
- On the other hand, taking into account that severe damages may arise for the data subjects in the process of the location data of persons by associating them with their health conditions, relevant institutions and organizations should take all necessary **technical and administrative measures** to ensure the security of the personal data, and also it should not be forgotten that the personal data will be erased or destructed in the event that the reasons for the processing no longer exist.

2. Sharing of health data with health authorities and institutions

Pursuant to the third paragraph of Article 6 of the Turkish Personal Data Protection Law No. 6698, "Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person that have confidentiality obligation or authorised public institutions, for the purposes of protection of public health, preventive medicine, medical diagnosis, treatment and nursing services, planning and management of healthcare services as well as their financing."

Also under Article 8 of the Turkish Personal Data Protection Law, transferring health data between health institutions in Turkey may take place in case one of the following conditions is met;

- Explicit consent of the data subject; or
- Third paragraph of Article 6 of the Law provided that sufficient measures are taken.

Nevertheless, the provisions of other laws relating to transfer of personal data are reserved.

So, processing of health data lawfully in Turkey does not mean that the data can be directly transferred to the third parties, Conditions set out in the third paragraph of Article 6 of the Law are to be fulfilled for transferring personal health data, if that health data will be shared without explicit consent. In this context, health data can be shared among health authorities and institutions in our country within the scope of combatting Covid-19.

Regarding this sharing arrangement, the Turkish Personal Data Protection Authority of Turkey has a regulatory and supervisory role. After exhausting the remedy of the

request to the data controller, the data subject may lodge a complaint with the Authority. The Authority can also make examination ex officio where it has learnt about alleged infringement.

In accordance with the decision of the Personal Data Protection Board dated 31/01/2018 and numbered 2018/10 regarding the "Adequate Measuresto be Taken by Data Controllers in the Processing of Personal Data of Special Categories", the minimum measures to be taken within the scope of this data processing activity have been determined by the Turkish Personal Data Protection Authority.

3. Sharing of health data with law enforcement agencies

Within the scope of Life Fits Into Home (HES) application, the Ministry of Health of Turkey shares the identity, contact and location data of users who violate self-isolation, with the Ministry of Interior and law enforcement agencies for the purpose of protecting public health and fight against the pandemic, while personal health data are not shared.

Regarding this sharing arrangement, the Personal Data Protection Authority of Turkey has a regulatory and supervisory role. After exhausting the remedy of the request to the data controller, the data subject may lodge a complaint with the Authority. The Authority can also make examination ex officio where it has learnt about alleged infringement.

4. Sharing of health data with charitable or other similar organisations

NIL.

5. Handling of employee data in work-from-home / return-to-work situations

Turkish Personal Data Protection Authority has published a public announcement regarding this issue.

Frequently asked questions and answers section has been prepared in this public announcement. Accordingly, the following questions have been answered:

- Can a healthcare organization contact individuals in relation to Covid-19 without having prior permission?
- It is known that more of the employees work from home during the pandemic. What kind of security measures should be taken during this period? Can an employer explain to colleagues / other employees that an employee has a virus?

- Can an employer disclose to her/his colleagues/other employees that an employee is infected with the virus? Can the health information of employees for public health be shared with authorities by the employer?
- Can an employer request all employees and visitors to provide information about their travels to affected countries and if they have viral symptoms, such as fever?
- Can an employer share the health data of the employers with authorities for public health purposes?

Source: https://www.kvkk.gov.tr/Icerik/6731/PUBLIC-ANNOUNCEMENT

United Kingdom - Information Commissioner's Office (ICO)

1. Contact tracing and location tracking

The UK has adopted both digital and manual contact tracing measures. A Bluetooth proximity app has been successfully launched in Northern Ireland, whilst a similar app is in development for the rest of the UK. Both apps use a 'decentralised' model and utilize the Apple/Google API. The NI app is interoperable with the Republic of Ireland's proximity app.

All UK nations have a manual contact tracing scheme, which collects names and contact details of individuals who have potentially been in contact with an infected person. Hospitality venues collect names and phone numbers on a voluntary basis to support this.

From the outset of the pandemic, the devolved Northern Ireland government sought expertise from the ICO about data protection expectations when developing their app. Engagement was constructive, transparent and frequent. The office provided advice, guidance and support to the DoH while maintaining the ICO's independent regulatory function.

The ICO has also engaged consistently with central UK government on the development of their app, though this is at an earlier stage of development and is yet to launch.

The NI government used the ICO's 'COVID-19 Contact tracing: data protection expectations on app development' guidance as the specification for their app. Privacy by design was incorporated through measures including data minimization, use of a decentralized model, a commitment to transparency and by providing a clear lifespan for the app. A Steering Committee has been formed to provide external oversight of the app and its governance. The Committee will guard against function creep, ensure the DPIA is kept up to date and manage the eventual winding down of the app.

The ICO has yet to review the final version of the UK-wide app. However, it has provided regular feedback to Government and the NHS by providing feedback on their DPIAs.

In some circumstances, controllers are required to consult the ICO before commencing processing. Neither Government felt that they were legally obliged to do so under the GDPR. However, both chose to consult with the ICO proactively. The ICO has therefore been engaging with both regularly in an advisory capacity, given the expertise as the data protection regulator, without prejudice to any future intervention by the Commissioner in accordance with her tasks and powers.

To promote good practices on the use of the contact tracing or location tracking measure, the ICO published a blog highlighting some high level design principles for authorities looking to implement tools based on the Bluetooth protocols. This was accompanied by a formal Opinion on the Google Apple API.

The ICO also published an "expectations document" containing 10 principles and 32 design considerations for Bluetooth protocol developers to be aware of when considering the whole data lifecycle and compliance with data protection legislation.

2. Sharing of health data with health authorities and institutions

Healthcare organizations are required to comply with a direction from the Secretary of State (Department of Health) to share confidential health information for the purposes of managing the response to the COVID pandemic.

The health data sharing requirement is outlined in the Health Service (Control of Patient Information) Regulations 2002 which sets aside the duty of confidence for organizations and public bodies processing confidential information.

For COVID-19 purposes this could include but is not limited to:

- understanding COVID-19 and risks to public health, trends in COVID-19 and such risks, and controlling and preventing the spread of COVID-19 and such risks;
- identifying and understanding information about patients or potential patients with or at risk of COVID-19;
- delivering services to patients, clinicians, the health services; and
- research and planning in relation to COVID-19.

The Control of Patient Information (COPI) notices apply to the period outlined by the Secretary of State in the notice. Any processing using the notices as a lawful basis must cease at the end of the period unless a legitimate alternate lawful basis can be found. The COPI regulation sits outside the ICOs regulatory purview to some extent, though it is referred to frequently due to its interaction with UK common law - a requirement

of UK data protection legislation is that the processing of personal data is otherwise lawful.

The ICO has also produced guidance covering data sharing during the pandemic: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/community-groups-and-covid-19/ ; https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/health-social-care-organisations-and-coronavirus-what-you-need-to-know/ .

The key messages are-

- to be clear, open and honest about what you are doing with personal data;
- to keep sharing data where it is necessary;
- to ensure sharing is lawful (with examples of lawful bases in layman's terms, such as it being within a person's reasonable expectations, with their consent or in their vital interest);
- to only share the minimum data necessary; and
- to keep a record of what has been done.

3. Sharing of health data with law enforcement agencies

There is no requirement, arrangement or plan in the U.K. on sharing of health data with law enforcement agencies for fighting COVID-19.

4. Sharing of health data with charitable or other similar organisations

The Covid-19 Public Health Directions 2020 were produced via provisions in the Health and Social Care Act 2012 on 17 March 2020. On the same day, a notice was issued under The Health Service (Control of Patient Information) Regulations 2002. Amongst other things, these required central government departments to collect, analyse and disseminate information about patients classified as clinically extremely vulnerable to the effects of Covid-19. Data already held by government combined with information provided by GP practices led to the Shielded Patients List (SPL), which is updated regularly.

The National Shielding Programme was established to protect clinically extremely vulnerable people from coming into contact with coronavirus by minimising interaction between themselves and others. Using the SPL, local authorities worked to identify people at a high risk and take action to support them whilst they were shielded. This included arranging for deliveries of medical supplies, free food parcels, and other types of essential care to those most in need. As well as using volunteers to

achieve this, supermarkets were brought in to support the government programme, although the SPL itself was not shared with them.

The National Shielding Programme's use of the SPL will necessarily end when the COPI notice expires. This was originally planned to be 30 September 2020 but has since been extended to 31 March 2021.

Regarding this data sharing arrangement, the ICO has provided data protection advice to controllers in order to enable them to respond at pace, and in compliance with data protection law.

The ICO has also produced guidance covering data sharing during the pandemic. Please refer to section 2 for details.

5. Handling of employee data in work-from-home / return-to-work situations

There were two major privacy issues identified in relation to handling of employee data in work-from-home / return-to-work situations:

- the rapid uptake of video conferencing software; and
- ensuring the security and confidentiality of personal data in work from home scenarios

The ICO responded to these issues through the publication of best practice advice on the coronavirus hub section of our website. This had four components:

- A security checklist for employers. The checklist gave advice on 'bring your own device' (BYOD), cloud storage, remote desktop, remote applications and email;
- More detailed and specific advice about BYOD considerations;
- Ten top tips for employees. This comprised some basic security advice around the security of paper records, the importance of security digital methods and ensuring that work and personal information are kept separate; and
- A blog providing advice on video conferencing software.

Our homeworking advice can be accessed here: *https://ico.org.uk/for-organisations/working-from-home/*

The ICO has also investigated a number of COVID- related cases, some of which involved homeworking scenarios. For example, the ICO has investigated an incident where homeworkers shared personal information on public platforms such as Facebook. The ICO has raised enquiries to such types of incidents. No case has yet met the threshold for enforcement action.

GPA COVID-19 Taskforce
Survey on Relevant Experience and Good Practices in Response to COVID-19

Background

Recognising the privacy and data protection challenges posed in the context of the COVID-19 pandemic, the GPA Executive Committee agreed in April 2020 to establish the new GPA COVID-19 Taskforce to address the emerging privacy issues posed by the spread of the virus.

One of the planned deliverables of the Taskforce is a **Compendium of Good Practices in Response to COVID-19**. The Compendium will contain relevant experience and good practices contributed by members and observers of GPA. It will be presented at the GPA virtual meeting in October 2020.

The objective of this survey is to collect relevant information for compiling the Compendium. The information collected focusses on those privacy issues identified as the most pressing in the survey conducted by the Taskforce amongst the GPA community in June 2020. Your authority / organisation is cordially invited to contribute to the Compendium by answering the following questions on or before **10 September 2020**. Please submit your responses to [redacted] of the Privacy Commissioner for Personal Data, Hong Kong, China (email: [redacted]).

It is **not necessary to answer all the questions** in the questionnaire below. If your authority / organisation has no relevant experience, or if your authority / organisation considers it inappropriate to share the experience (because of, for example, confidentiality), please state the fact and skip the question(s). Please

answer the questions to the best of your knowledge, i.e. if there are plans for your jurisdiction to adopt and/or implement any measures relating to the questions below in the near future, please also state the same as far as you know.

To facilitate the compilation of the Compendium, you are requested to keep your responses succinct, and **limit the number of words for the response to each of the five issues below to 500**.

Name of your authority: _____
Jurisdiction: _____

Please also insert the logo of your authority or a photograph of your Commissioner:

1. Contact tracing and location tracking

(a) If your jurisdiction adopted contact tracing or location tracking measures aimed at containing the spread of COVID-19, please provide a brief description of the measures. You may wish to include the following information, as appropriate:

- for digital measures:
    - the names and developers of the measures;
    - how the digital measures work;
    - the underlying technology employed, for example, the use of Bluetooth technology;
    - whether the digital measures are intended to supplement manual contact tracing;

- for both digital and manual measures:
    - what kinds of data will be collected;
    - how or whether the measures are clinically relevant and necessary;
    - how the data will be used;
    - to whom the data will be usually disclosed to; and/or
    - whether it is voluntary or mandatory.

[For jurisdictions adopting a digital contact tracing or a location tracking digital measure, please answer sub-questions (b), (c), (d) & (e). For jurisdictions that do not adopt digital measure, please answer sub-questions (d) & (e).]

(b) If your jurisdiction has adopted a digital contact tracing or a location tracking digital measure aimed at containing the spread of COVID-19, did the developers of such digital measure engage in an open and constructive engagement with your authority / organisation? If so, please describe your authority / organisations' experience in further detail.

(c) Was a privacy by design approach taken to develop the digital measure? In your response, you may wish to include:

- whether in developing the application, an assessment of privacy risks was taken;
- how developers have addressed matters of data security and safeguards employed to protect data collected by the digital measure. This may include technical measures such as privacy and security settings/features or through external measures such as enshrining privacy protections in legislation. If privacy protections are enshrined in legislation, please describe the key features of the legislation including any enforcement powers;
- whether there are notification requirements regarding the improper access to the data;
- whether there will be a mandatory review of the digital measure (for instance, of the efficacy of the digital measure and technology employed, or the collection and storage of the data);
- whether there are penalties that apply to the improper use and access to the data, including how these might be enforced; and/or
- whether the digital measure is temporary and whether data collected by the digital measure (e.g. contact tracing application) will be deleted when no longer required.

(d) What is the role of your authority / organisation in the planning for and implementation of the contact tracing or a location tracking measure? In your response, you may wish to include:

- whether your authority / organisation was consulted on personal data protection related issues; and/or
- any roles that have been conferred to your authority / organisation in relation to the measure, such as a regulatory or oversight role.

(e) What are the good practices and effective policies promoted by your authority / organisation or implemented by the relevant data users / controllers in your jurisdiction on the use of the contact tracing or location tracking measure. This may include, but is not limited to:

- conducting a privacy impact assessment;
- advocating for the minimisation of the collection of personal data;
- advocating for use and disclosure limitations, and/or transparency requirements; and
- monitoring the efficacy of digital contact tracing or location tracking measure.

Please elaborate. Please also provide links to the relevant publications, where available.

2. Sharing of health data with health authorities and institutions

(a) Is there any requirement, arrangement or plan in your jurisdiction on sharing of health data with health authorities and institutions for fighting COVID-19? (Yes / No)

(b) If yes, please provide a brief description of the requirement, arrangement or plan (e.g. what kinds of health data will be shared; how the data will be shared)?

(c) What is the role of your authority / organisation in the data sharing arrangement or plan?

(d) What are the good practices promoted by your authority / organisation in relation to data sharing with health authorities and institutions? Please elaborate.

(e) Will data be retained for research in the public interest? If so-

- Are there any limitations on the retention of data?
- What privacy protections have been adopted and is the anonymisation of data envisaged?

3. Sharing of health data with law enforcement agencies

(a) Is there any requirement, arrangement or plan in your jurisdiction on sharing of health data with law enforcement agencies for fighting COVID-19? (Yes / No)

(b) If yes, please provide a brief description of the requirement, arrangement or plan?

(c) What is the role of your authority / organisation in the data sharing arrangement or plan?

(d) What are the good practices implemented or promoted by your authority / organisation in relation to data sharing with law enforcement agencies? Please elaborate.

4. Sharing of health data with charitable or other similar organisations

(a) Is there any requirement, arrangement or plan in your jurisdiction on sharing of health data with charitable or other similar organisations for offering support and assistance to those in need amidst the COVID-19 pandemic? (Yes / No)

(b) If yes, please provide a brief description of the requirement, arrangement or plan?

(c) What is the role of your authority / organisation in the data sharing arrangement or plan?

(d) What are the good practices implemented or promoted by your authority / organisation in relation data sharing with charitable or other similar organisations? Please elaborate.

(e) Will data be retained for research in the public interest? If so, are there any limitations on the retention of the data? What privacy protections have been adopted and is the anonymisation of data envisaged?

5. Handling of employee data in work-from-home / return-to-work situations

(a) What are the major privacy issues identified by your authority / organisation in relation to handling of employee data in work-from-home / return-to-work situations?

(b) What are the good practices promoted by your authority / organisation in addressing or mitigating the privacy issues associated with the handling of employees' personal data in work-from-home/return-to-work situations? Please elaborate.

(c) Have there been any complaints, breaches, or investigations related to the handling of employee data in work-from-home / return-to-work situations, and how has your authority / organisation responded to this?

- End -