Global Privacy Assembly 2020 (Virtual)

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

14 October 2020

Ada CHUNG Lai-ling, Barrister
Privacy Commissioner for Personal Data,
Hong Kong, China

PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

GPA COVID-19 Taskforce

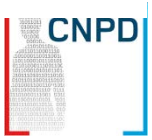
- Established in May 2020 by the Executive Committee of GPA
- Chaired by Privacy Commissioner Raymund Liboro, NPC Philippines
- Objectives:

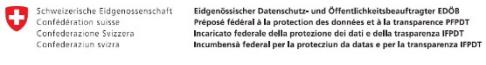
  To drive practical responses to privacy issues emerging from the COVID-19 pandemic, and assist GPA membership with insight, best practices and the delivery of capacity building activities.

Survey on Relevant Experience and Best Practices in Response to COVID-19

32 GPA members and observers responded to the Survey:

(by alphabetical order of the country / jurisdiction names)



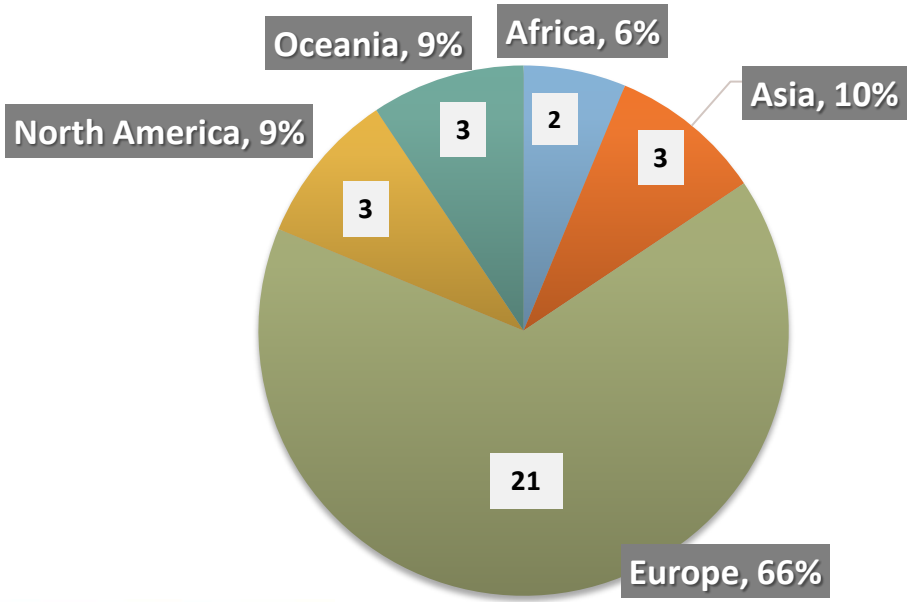


Five Topics Covered in the Survey

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

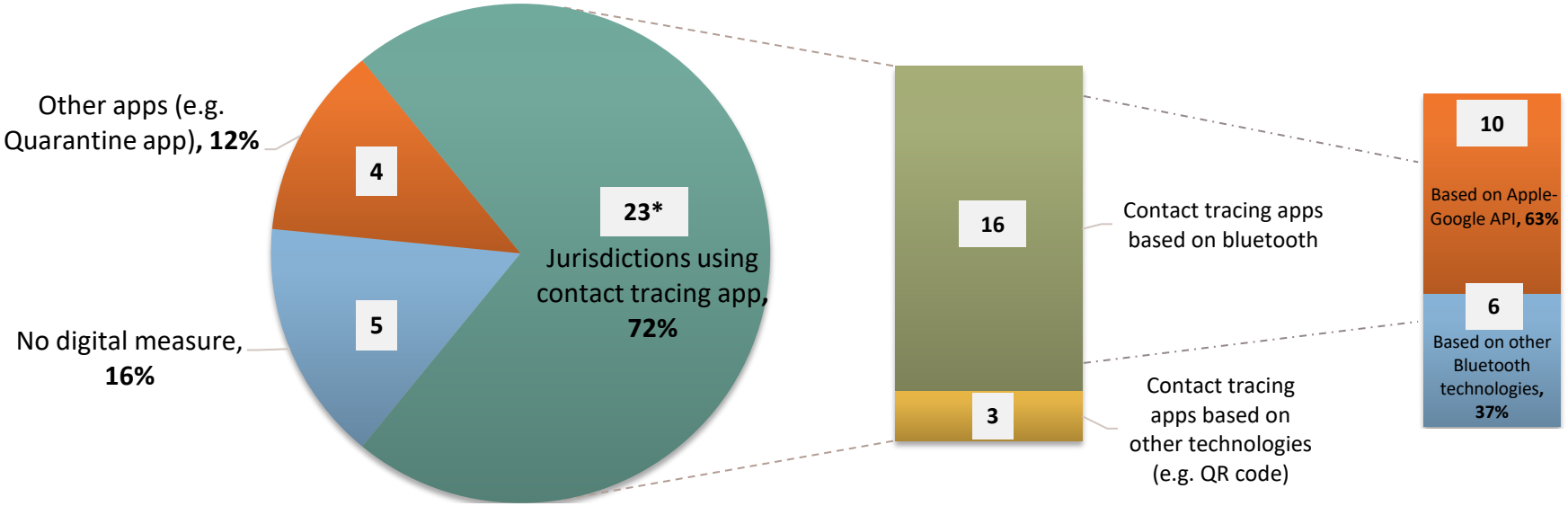
Survey on Relevant Experience and Best Practices in Response to COVID-19

Geographic distribution of the responses (Total: 32)



(1) Contact tracing and location tracking

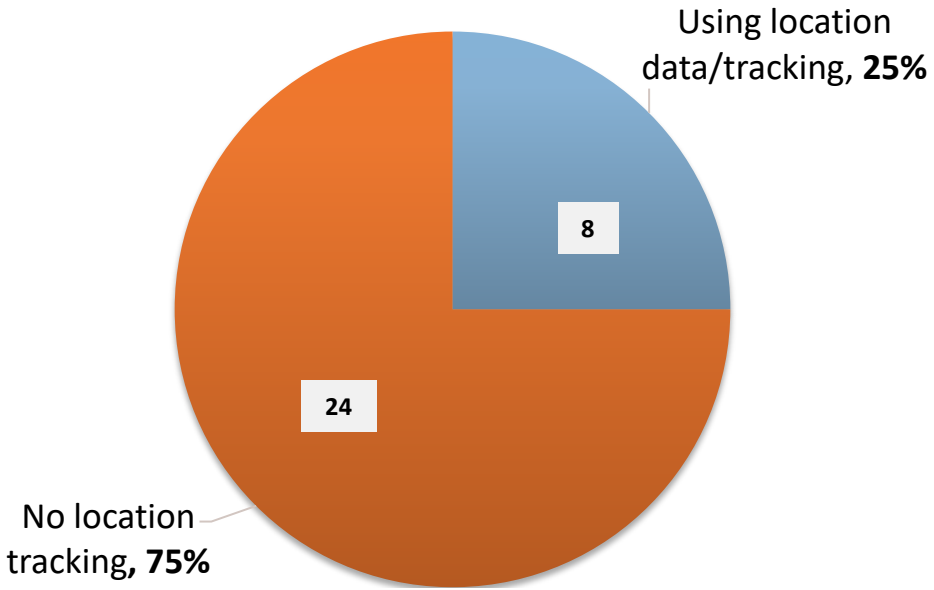
Jurisdictions' use of digital contact tracing measures



** Only 19 jurisdictions had their own contact tracing apps. Liechtenstein recommended individuals to use the contact tracing app of Switzerland. The same contact tracing apps used across the country in Australia and Canada.*

(1) Contact tracing and location tracking

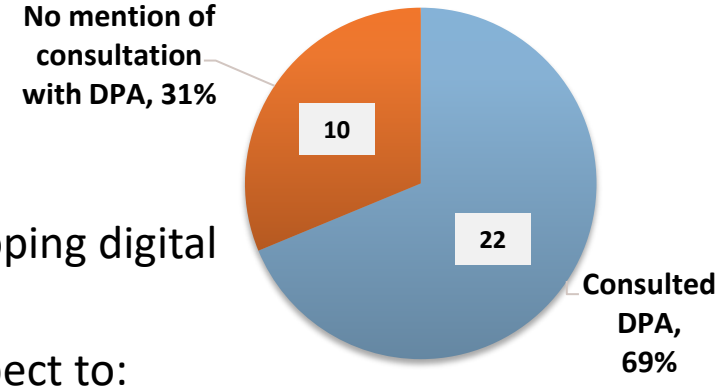
Jurisdictions' use of location tracking*



*Among all 32 jurisdictions

(1) Contact tracing and location tracking

Constructive engagement with DPAs



- High engagement with DPAs in the process of developing digital contact tracing measures
- 22 jurisdictions (69%) consulted their DPAs with respect to:
  - Data protection / privacy impact assessments
  - Other general privacy issues
- Some DPAs participated in special taskforce or committees for the developing of contact tracing apps, or held direct discussion with the app developers

(1) Contact tracing and location tracking

Legislative amendments

Laws addressing privacy concerns

Australia: Amendments to the Privacy Act 1988 prohibit compulsory use of COVIDSafe app, etc.

Netherlands: Legislation under discussion in Parliament to prohibit the use of contact tracing app as a pre-condition to access to building and services, etc.

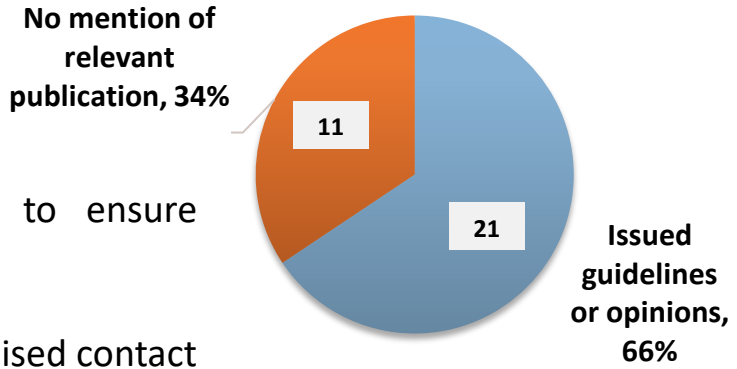
Laws facilitating the use of data

Slovakia: Created new legal basis for personal data processing for digital contact tracing

Bulgaria: Amended law to obligate collection of location data of persons violating confinement order

(1) Contact tracing and location tracking

Best practice recommendations by DPAs (Non-exhaustive)

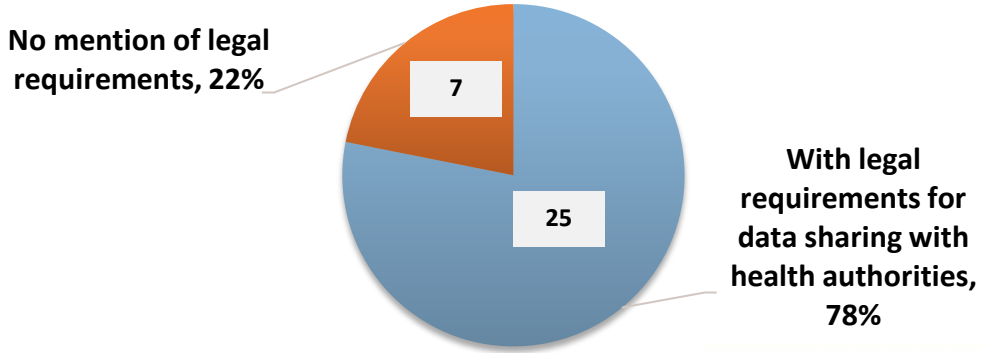


- Conducting data protection/privacy impact assessments to ensure **Privacy by Design**
- **Voluntary adoption** of digital contact tracing measures
- **Data minimisation**: de-identification of data, use of decentralised contact tracing model
- Enhancing **transparency & public trust**: publishing privacy policies of the apps, opening up the source code of the apps, informing the users when their data is deleted, chartering DPAs or oversight committees to review the operation of the apps
- **Specifying data retention periods**
- **Decommission contact tracing apps** as soon as the pandemic is over
- **Continuous assessment** of the efficacy of contact tracing apps

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

Legal requirements

- Most of the DPAs **(25 out of 32, 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.
- Some were **specifically in response to COVID-19** (e.g. Australia and Hong Kong)



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

Retention of data by health authorities

Retention periods of health data collected by health authorities vary across jurisdictions:

Jurisdiction	Types of data	Retention period
Jersey	Contact tracing data	21 days
Belgium	Health and contact tracing data	60 days
Andorra	Health data	As long as there is a reasonable purpose
Philippines	Health and contact tracing data	As long as it is necessary for contact tracing
Netherlands	Health data	Up to 5 years
New Zealand	Health data	Minimum of 10 years

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

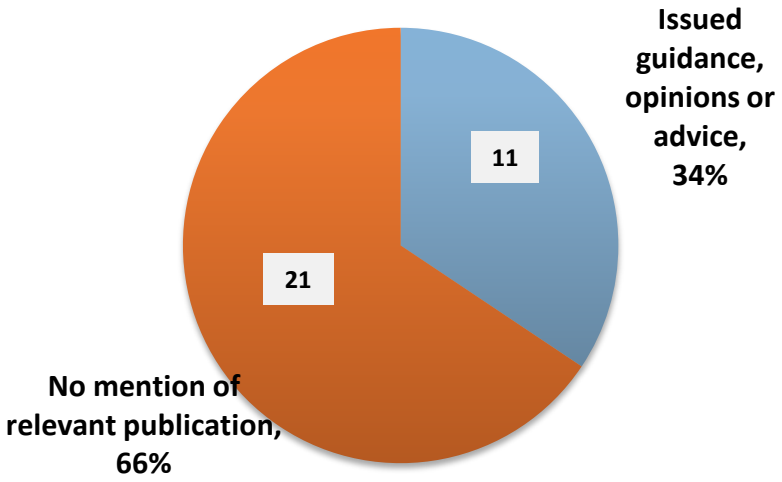
Retention of data for research

- 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)

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

Roles of DPAs

- **<u>11</u>** out of 32 DPAs **issued guidance, opinions or advice** on the processing of health data during the COVID-19 pandemic
- Some DPAs had **deeper involvement**, e.g.
  - Be informed of any planned initiatives that may have impact on privacy (OPC Canada)
  - DPA's opinion has to be sought before data sharing arrangement is implemented (San Marino DPA)



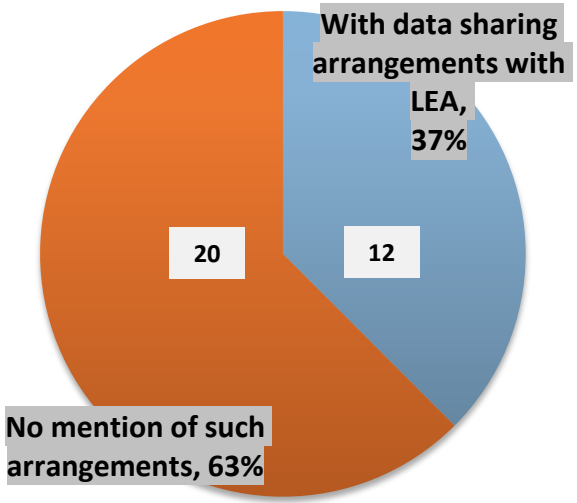
(2) Sharing of health data with health authorities and institutions

Best practice recommendations by DPAs (Non-exhaustive)

- Conducting data protection / privacy impact **assessment** and ethical **evaluation**
- **Prior consultation** with DPAs
- Defining the **purposes** of data sharing
- Defining the specific **kinds of personal data** to be shared
- Sharing **anonymised / de-identified** data, where possible
- Entering into **written data sharing agreements**
- Limiting **secondary uses** and onward transfer of the health data
- Adopting adequate and proportionate **data security measures**
- Being **clear, open and honest** about the sharing of health data
- Keeping **proper records** about the data sharing
- **Destroying the data** after the sharing purposes are fulfilled

(3) Sharing of health data with law enforcement agencies

- **<u>12 DPAs</u>** stated there were **laws, regulations or other arrangements** that enable data sharing with law enforcement agencies for combating COVID-19
- Enabled by:
  - **Existing legal frameworks,** e.g. exemption under personal data protection laws and general investigation powers of law enforcement agencies (e.g. Albania, Canada, Germany, Hong Kong, Japan, Newfoundland and Labrador, Slovakia)
  - **New regulations/arrangements** in time of COVID-19 (e.g. Georgia and the Philippines)
- Most common reason for data sharing: **enforcing quarantine orders** (e.g. Georgia, Newfoundland and Labrador and Slovakia)



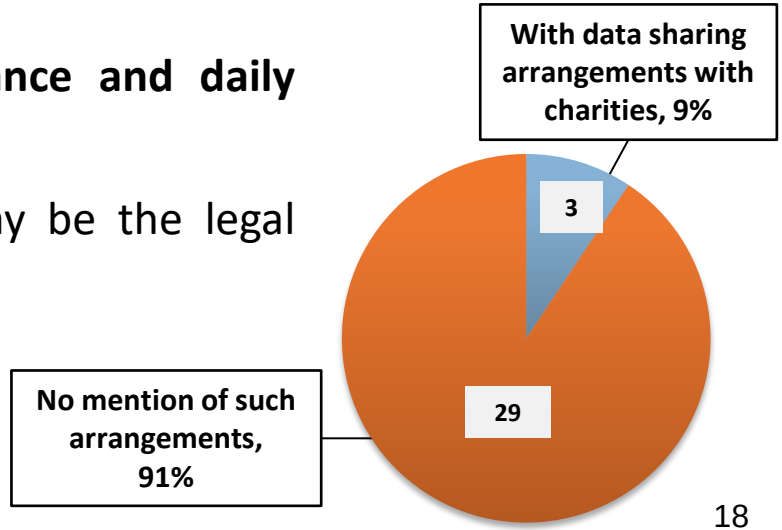
(3) Sharing of health data with law enforcement agencies

Data Sharing of contact tracing app data with law enforcement prohibited in Australia

- 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

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

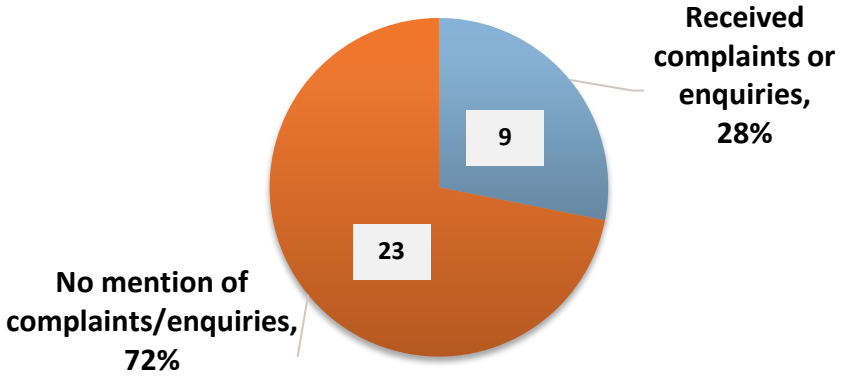
- **Uncommon**: only **3** DPAs were aware of (possible) data sharing arrangements with charities in their jurisdictions
  - i.e. Burkina Faso, Finland and the UK
- Main purpose of data sharing: **Providing assistance and daily essentials** to COVID-19 patients in need
- **Public interest** and **the need to protect lives** may be the legal bases for data sharing (e.g. Canada, Japan)



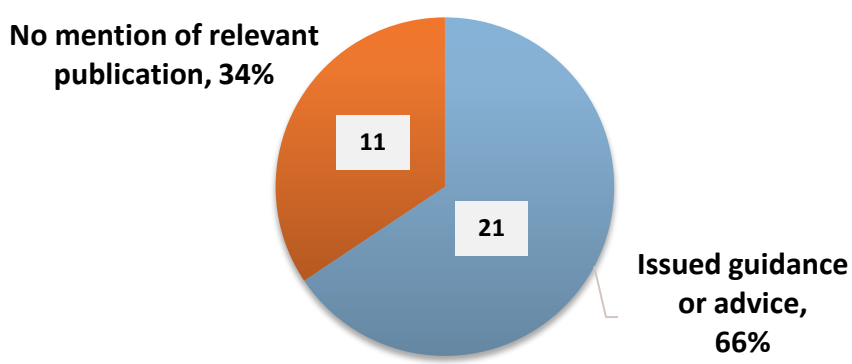
(5) Handling of employee data in work-from-home or return-to-work situations

Experience of DPAs

9 out of 32 DPAs (28%) had received complaints or enquiries relating to work-from-home or return-to-work situations



21 out of 32 (66%) DPAs stated that they had issued related guidance or advice



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

Data security and privacy issues in work-from-home situations

a. 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 handling of **paper files**

g. Difficulty in ensuring that **data processors** adhere to the same data protection standards

h. Increased **risk of data breach** due to deviation from standard processes

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

Work-from-home best practices for employers

a. Conducting **risk assessments**, considering the changes in the work arrangements
b. Developing **internal policies** and conveying them clear to employees
c. Ensuring reasonable steps being 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 out from and returned to office premises
h. Ensuring **appropriate control** over how external service providers will handle the data entrusted to them
i. Raising **employees' awareness** on phishing and social engineering attacks (especially COVID-19 related messages)
j. Requiring employees to **report data breaches** immediately

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

Work-from-home best practices for employees

a. Following **policies, procedures and guidance** of employers
b. Using **companies' devices** where possible
c. Using only hardware and software **approved by employers**
d. Ensuring **security of personal devices** 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 if necessary
k. **Turning off** microphones and cameras when not in use;
l. **Transferring** physical files **securely**, e.g. using cases with locks
m. **Keeping** work files at home **securely**, e.g. lock up paper files and electronic devices after work or when not in use, and encrypting electronic files
n. **Not mixing** employers' data with employees' own personal data
o. **Not disposing** work-related documents at home
p. Being vigilant about opening **web links and attachments** in emails or other messages
q. **Notifying employers** immediately in the event of data breach

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

Privacy issues in return-to-work situations

a. **Proportionality** regarding the **collection of personal data** from employees to combat COVID-19, in particular sensitive health data

b. **Security** of personal data collected from employees

c. **Allowable use and disclosure** of employees' personal data

d. **Retention period** of employees' personal data

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

Return-to-work best practices for employers

a. Collecting, using and disclosing **minimum amount of personal data** reasonably necessary to prevent or manage COVID-19, or for contact tracing

b. Adopting **self-reporting mechanism** 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 and disclosed in responding to potential or confirmed cases of COVID-19

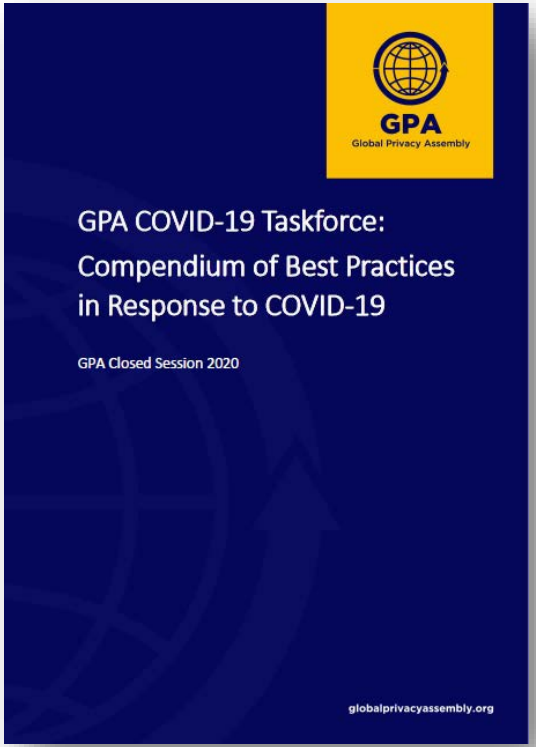
e. Ensuring reasonable steps are in place to safeguard the **security of personal data**

f. Disclosing only **employees' personal data when necessary**. E.g. disclosing to public health authorities only

g. **Destroying the personal data** once it is not reasonably necessary for contact tracing or related purposes, except there are legal obligations to retain

h. **Reviewing COVID-19 related initiatives regularly** and consider their necessity in light of the latest circumstances

The Compendium



Contact Us

www.pcpd.org.hk

Thank You!

PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong