個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data

Protecting Privacy and Building Trust for Community Resilience

Knowledge Event - Health System and Community Resilience:
Lessons From The COVID-19 Pandemic

4 December 2023

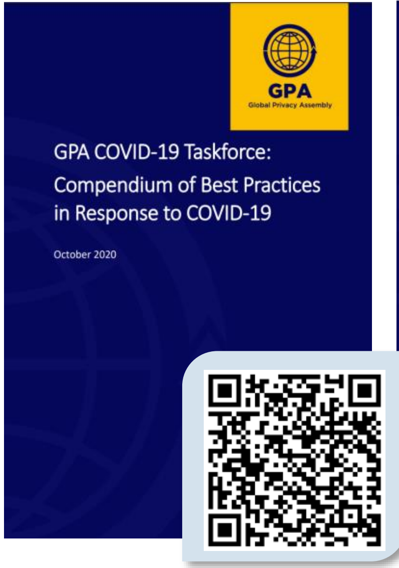
Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data, Hong Kong, China

Experience and Best Practices Around the World

Compendium of Best Practices in Response to COVID-19 (Part I & Part II)

Compiled by Hong Kong as a member of the COVID-19 Working Group of the Global Privacy Assembly:

- Conducted surveys among data protection authorities worldwide (DPAs)
- Explored pressing data protection and privacy issues which arose during the pandemic
- Collected the relevant experience and best practices in dealing with data protection/privacy issues

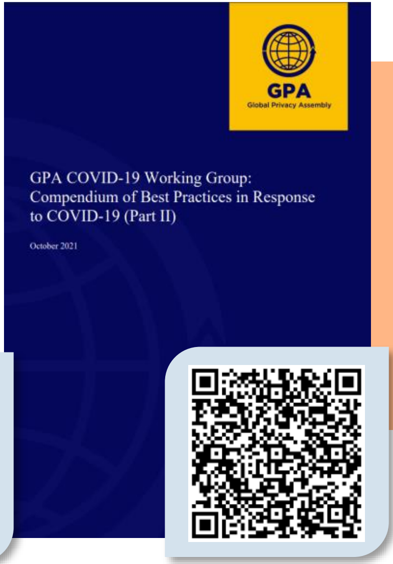


GPA
Global Privacy Assembly

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

October 2020

Issued in Oct 2020



GPA
Global Privacy Assembly

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

October 2021

Issued in Oct 2021

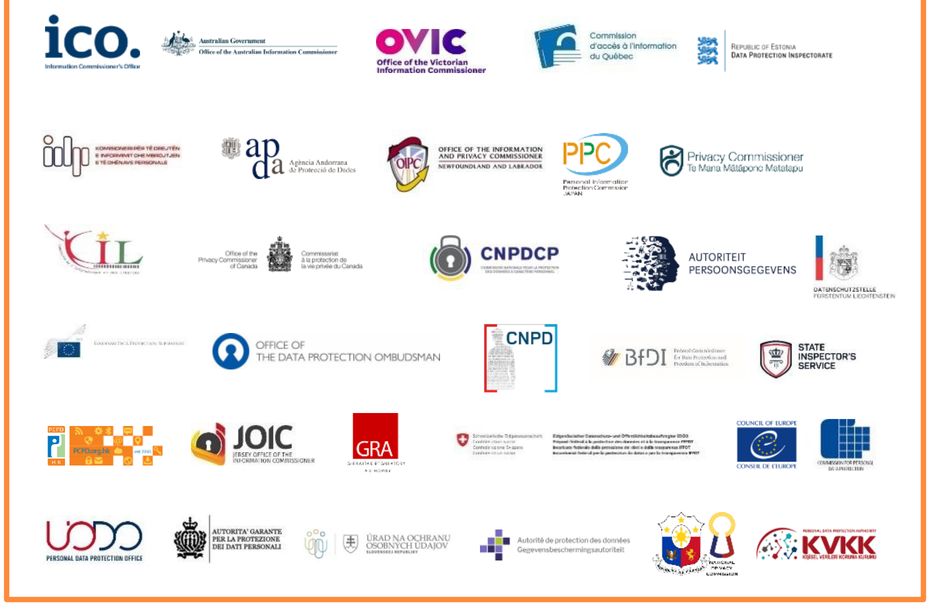
Global Privacy Assembly (GPA)

The leading international forum for over 130 data protection authorities from around the globe to discuss and exchange views on privacy issues and the latest international developments.

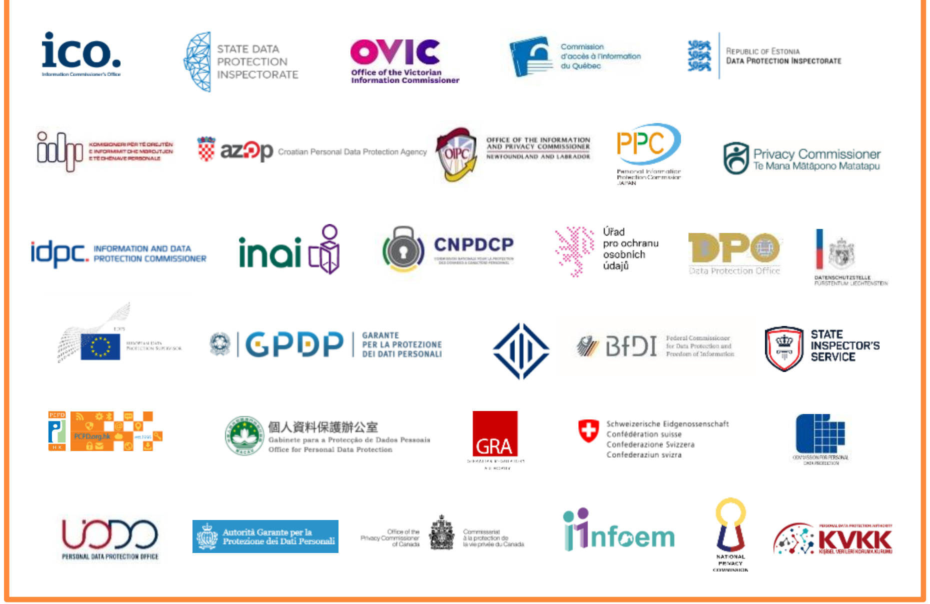
Surveys on Relevant Experience and Best Practices in Response to COVID-19

32 GPA members and observers responded to the Survey in both 2020 and 2021:

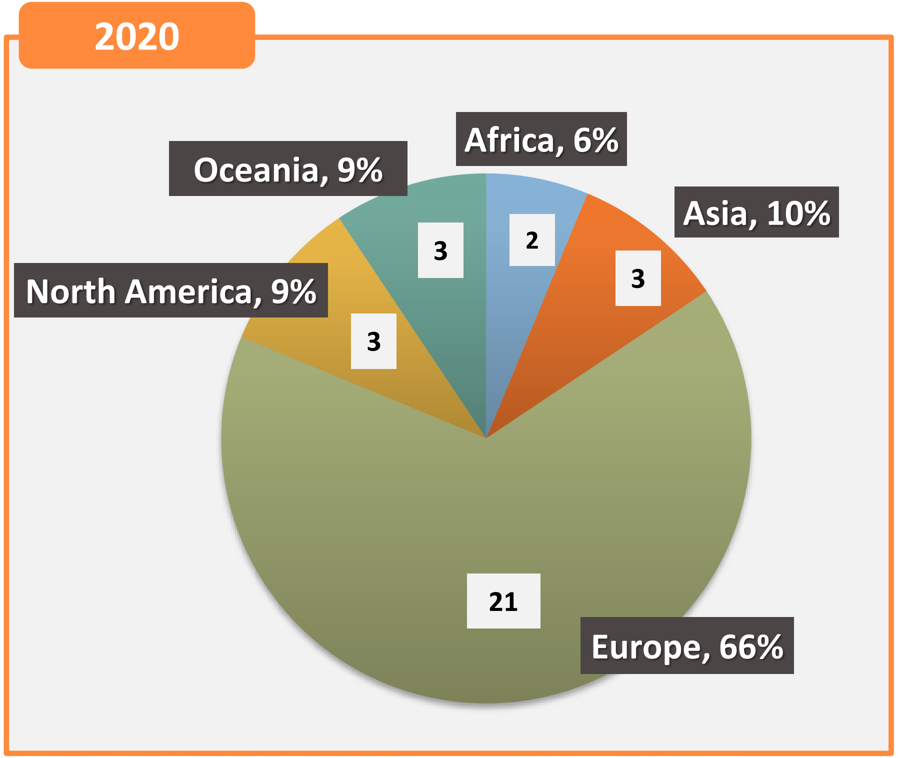
2020

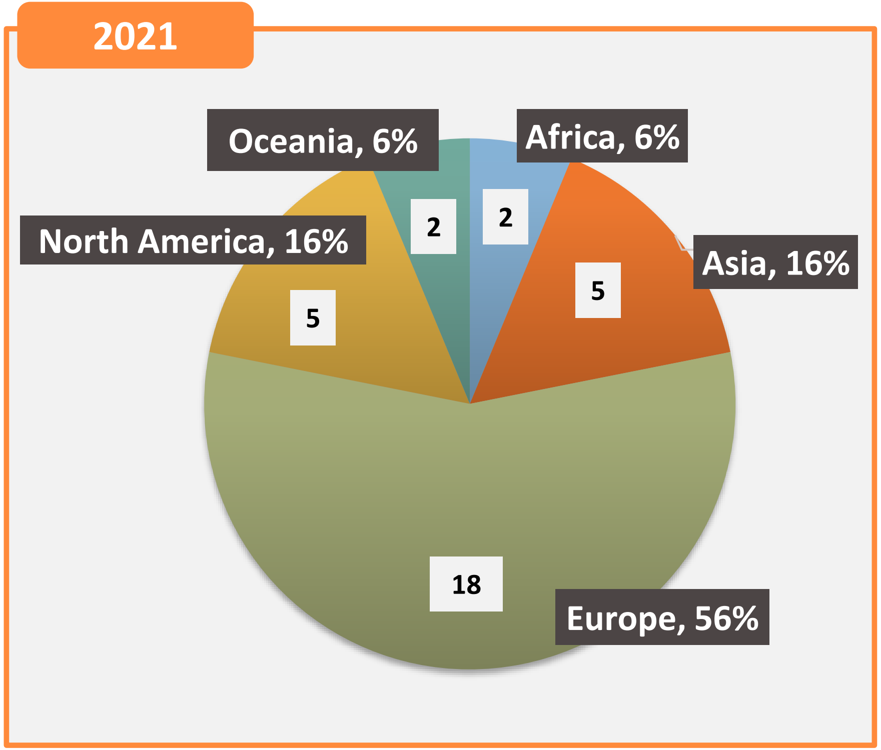

ico. Information Commissioner's Office
Australian Government Office of the Australian Information Commissioner
OVIC Office of the Victorian Information Commissioner
Commission d'accès à l'information du Québec
Republic of Estonia Data Protection Inspectorate
idp Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale
apda Agència Andorrana de Protecció de Dades
OIPC Office of the Information and Privacy Commissioner Newfoundland and Labrador
PPC Personal Information Protection Commission Japan
Privacy Commissioner Te Mana Mātāpono Matatapu
CIL
Office of the Privacy Commissioner of Canada Commissariat à la protection de la vie privée du Canada
CNPDCP
Autoriteit Persoonsgegevens
Datenschutzstelle Fürstentum Liechtenstein
European Data Protection Supervisor
Office of the Data Protection Ombudsman
CNPD
BfDI Federal Commissioner for Data Protection and Freedom of Information
State Inspector's Service
PCPD.org.hk
JOIC Jersey Office of the Information Commissioner
GRA
Schweizerische Eidgenossenschaft
Council of Europe Conseil de l'Europe
Commission for Personal Data Protection
UODO Personal Data Protection Office
Autorità Garante per la Protezione dei Dati Personali
Úrad na ochranu osobných údajov Slovenskej republiky
Autorité de protection des données Gegevensbeschermingsautoriteit
National Privacy Commission
KVKK Kişisel Verileri Koruma Kurumu

2021


ico. Information Commissioner's Office
State Data Protection Inspectorate
OVIC Office of the Victorian Information Commissioner
Commission d'accès à l'information du Québec
Republic of Estonia Data Protection Inspectorate
idp Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale
azop Croatian Personal Data Protection Agency
OIPC Office of the Information and Privacy Commissioner Newfoundland and Labrador
PPC Personal Information Protection Commission Japan
Privacy Commissioner Te Mana Mātāpono Matatapu
idpc Information and Data Protection Commissioner
inai
CNPDCP
Úřad pro ochranu osobních údajů
DPO Data Protection Office
Datenschutzstelle Fürstentum Liechtenstein
European Data Protection Supervisor
GPDP Garante per la Protezione dei Dati Personali
BfDI Federal Commissioner for Data Protection and Freedom of Information
State Inspector's Service
PCPD.org.hk
個人資料保護辦公室 Gabinete para a Protecção de Dados Pessoais Office for Personal Data Protection
GRA
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Commission for Personal Data Protection
UODO Personal Data Protection Office
Autorità Garante per la Protezione dei Dati Personali
Office of the Privacy Commissioner of Canada Commissariat à la protection de la vie privée du Canada
infoem
National Privacy Commission
KVKK Kişisel Verileri Koruma Kurumu

Geographic Distribution of the Responses in 2020 and 2021

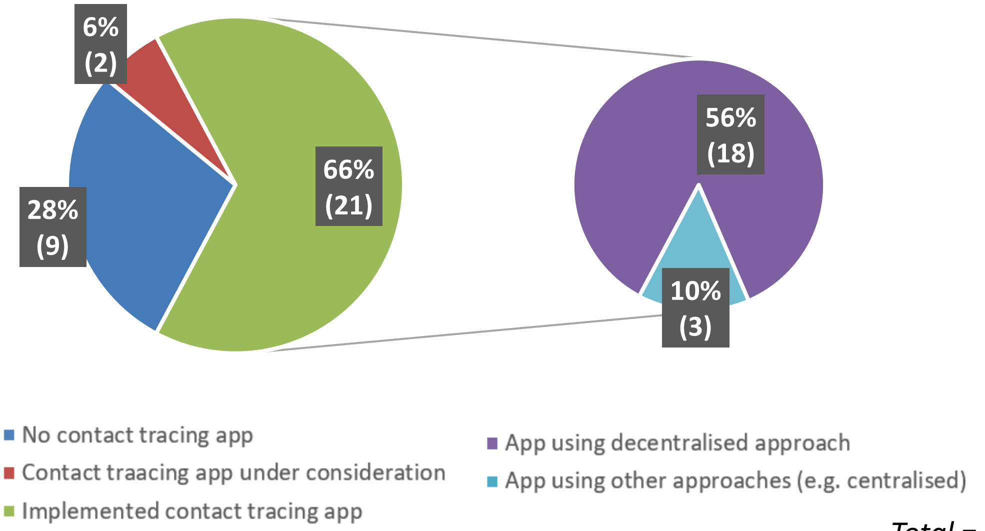




Prevalence of Contact Tracing Apps

From *Compendium Part II*

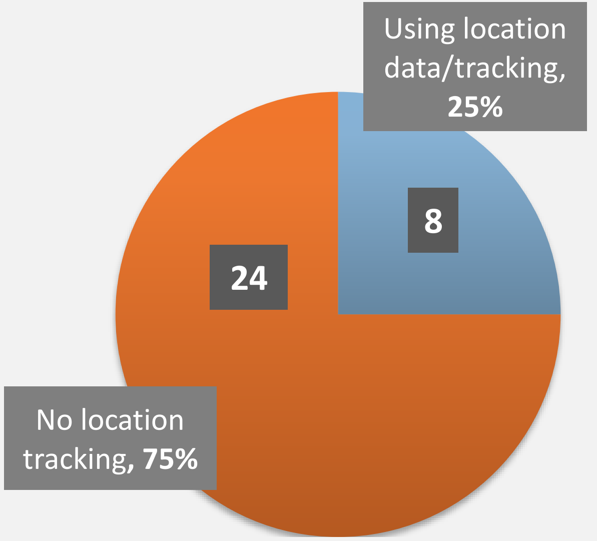
Jurisdictions With Contact Tracing Apps and Their Adopted Approaches



Total = 32

From *Compendium Part I*

Jurisdictions' Use of Location Tracking



Total = 32

Major Privacy Risks of Contact Tracing Measures

**non-exhaustive*

From *Compendium Part II*

1. Data Security Risks
2. Bluetooth Technology Related Privacy Risks
3. Re-identification of Individual Users
4. Excessive Collection of Personal Data
5. Unauthorised Processing and Disclosure of Sensitive Data
6. Reuse for Secondary Purposes

Contact Tracing App in Hong Kong

LeaveHomeSafe App

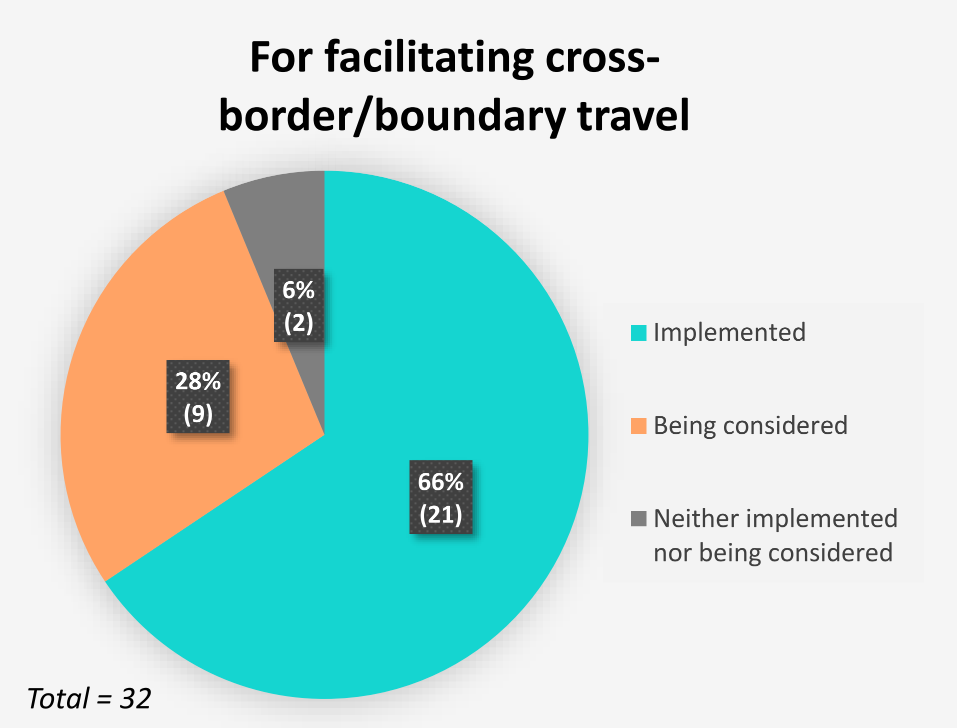
- Launched on 16 November 2020. Use of the App in certain types of premises became mandatory in late 2021.
- Citizens (unless exempted) were required to scan the venue QR code before they were allowed to enter the premises.
- Visit records of confirmed or suspected cases were regularly downloaded and matched against the user's visit records in their mobile phones.
- Notifications were sent to users who had visited a venue that a confirmed patient had also visited at about the same time
- Ceased operation on 8 January 2023

Good Privacy Practices Adopted in LeaveHomeSafe App

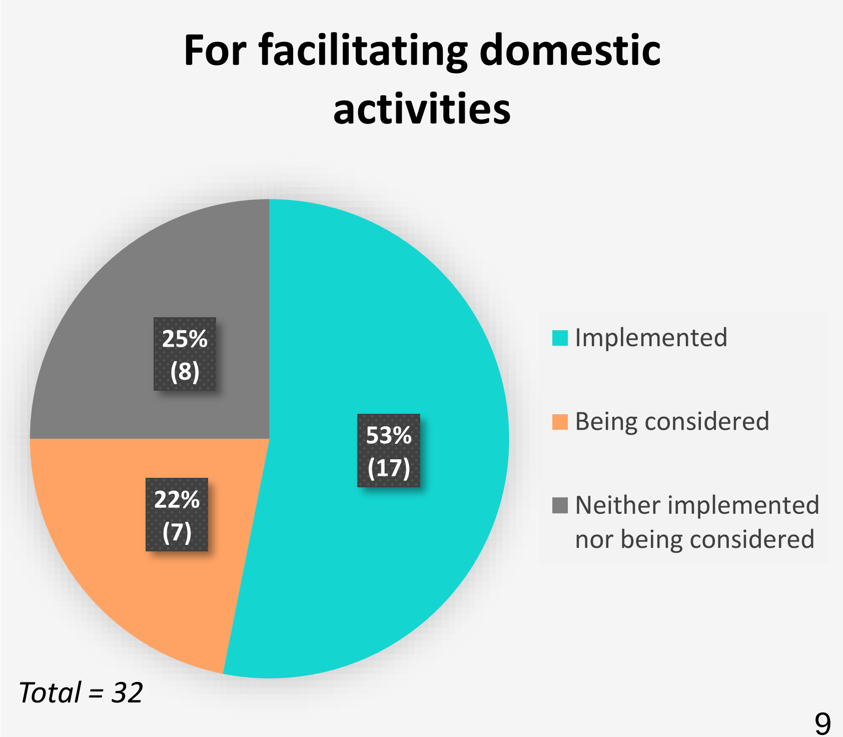
Relevant Data Protection Principles		Practices Adopted in LeaveHomeSafe App *non-exhaustive*
Data Minimisation	**Minimising Data Collection**	• No location tracking function, did not collect users’ GPS data • Did not require registration (no collection of personal data)
	Minimising Data Uploaded	• Visit records were kept on users’ smartphones only • Only in the event of a confirmed infection would the users’ visit records be uploaded for conducting epidemiological investigations
Strengthening Data Security		• Visit records were encrypted
Retention Limitation		• Visit records would be automatically erased after 31 days
Purpose Limitation		• All visit records uploaded were deleted when the operations ceased
Privacy by Design		• Conducted Privacy Impact Assessment before implementation

Prevalence of Health Passport

From *Compendium Part II*



Total = 32



Total = 32

Major Privacy Risks of Health Passports

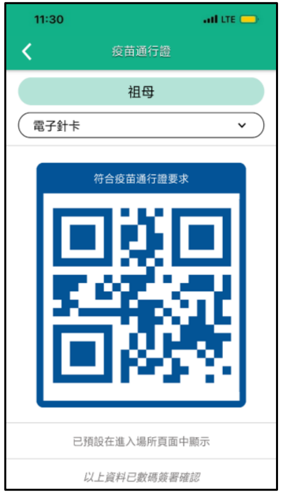
*non-exhaustive

From *Compendium Part II*

1. Data Security Risks
2. Forgery of Health Passports
3. Unnecessarily Displaying or Sharing Personal Data
4. Personal Data Retained for Longer than Necessary
5. Reuse for Secondary Purposes

Health Passport in Hong Kong

Vaccine Pass

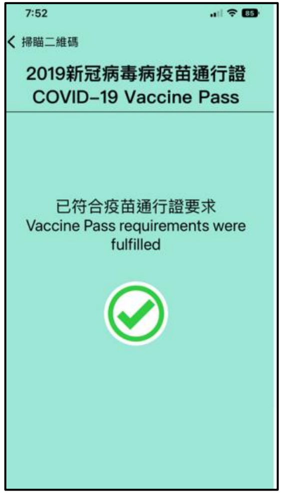


符合疫苗通行證要求

已預設在進入場所頁面中顯示

以上資料已數碼簽署確認

The vaccine pass could be stored inside the LeaveHomeSafe App



2019新冠病毒病疫苗通行證
COVID-19 Vaccine Pass

已符合疫苗通行證要求
Vaccine Pass requirements were fulfilled

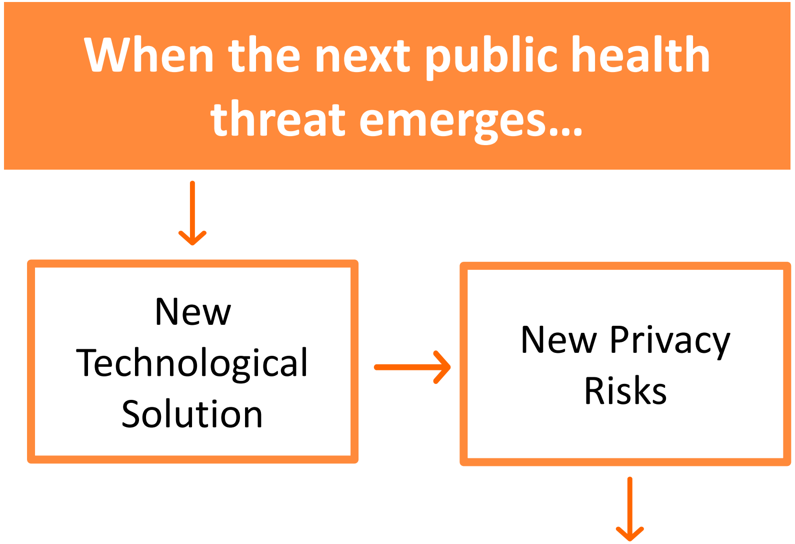
Screenshot of the "QR Code Verification Scanner" app

- Introduced on 24 February 2022
- Citizens were required to have received vaccination before entering certain types of premises (unless exempted)
- Vaccination records in paper or electronic format (affixed with a unique QR code indicating the vaccination status and test result) were required to be presented to premises operators
- Premises operators used a "QR Code Verification Scanner" app to scan the QR codes affixed on vaccination records for verification
- For the confirmed cases, their QR codes would be displayed in red, which restricted them from entering specified premises
- Vaccine Pass requirement was removed on 29 December 2022

Good Privacy Practices Adopted in Vaccine Pass

Relevant Data Protection Principles		Practices Adopted in Vaccine Pass *non-exhaustive
Data Minimisation	Minimising Data Disclosed	• Only a QR code was required to be presented to premises operators • When premises operators scanned visitor's vaccine pass, no personally identifiable information would be shown, only vaccination status
	Minimising Data Uploaded	• Visit records were kept on premises operators' apps only, in encrypted form • Only if a confirmed patient had visited the premises would visit records be uploaded for conducting epidemiological investigations
Strengthening Data Security		• Visit records stored containing personal data were unidentifiable after they were hashed & masked
Retention Limitation		• Visit records would be automatically erased after 31 days
Purpose Limitation		• Uploaded visit records were only used to conduct epidemiological investigations
Privacy by Design		• Conducted Privacy Impact Assessment before implementation

Looking Ahead



When the next public health threat emerges…

New Technological Solution

New Privacy Risks

How to apply the lessons learnt?

From the Compendium…

- ➢ Best Practices recommended by DPAs regarding contact tracing apps and health passports had many similarities
- ➢ Many were in line with conventional data protection principles

⚠ **Conventional data protection principles** are still applicable in future crisis in **striking the balance** between privacy protection and public health

Best Practices Recommended by DPAs (From *Compendium*)

For Contact Tracing Apps and Health Passports:

1 Data Minimisation

A Data Collection

- No location tracking or logging of individuals' activities
- Uploading only the information of infected persons to central database

B Disclosure of Data

- Masking personal data where possible
- Verifying individuals' health status through scanning QR codes/barcodes only

C Data Transfer to Third Parties

- Verification of individual's health status without transfer of personal data
- Using privacy preserving solutions (e.g. device level processing)

2 Strengthening Data Security

For Contact Tracing Apps:

- Implementing anonymisation measures

For Health Passports:

- Verifying the authenticity of vaccine/recovery certificate through cryptographic means
- Deleting personal data upon expiry of vaccine/recovery certificate

Best Practices Recommended by DPAs (From *Compendium*)

For Contact Tracing Apps and Health Passports:

③ Purpose Limitation

- Pledging to decommission the contact tracing/health passport app when the pandemic is over
- Prohibiting access to and subsequent use of personal data

④ Being Open and Transparent

- Disclosing the list of entities that have access to the personal data collected by the app(s)
- Where appropriate, making source code and technical specifications publicly available

⑤ Privacy by Design

- Conducting DPIA/PIA before rolling out
- Conducting regular audit and reassessment thereafter

Thank you

www.pcpd.org.hk

communications@pcpd.org.hk