Agenda

- Introduction
- Data Privacy Practices
  - Practising staff work-from-home arrangements
  - Enforcing vaccine pass requirements
  - Implementing surveillance measures at service venues
  - Collecting HKID card information from stakeholders
- Q&A

1. Work From Home Arrangements

Morgan Lewis

Key Questions for WFH Arrangements

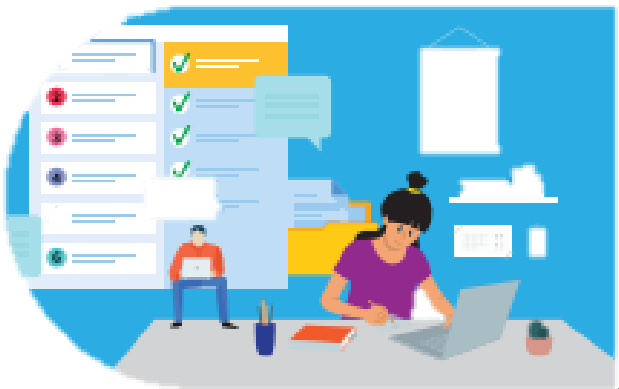
Can NGO staff members carry materials (hard copies or electronic data through laptops etc.) containing personal data back to their home? If this is not prohibited, what can staff members do to better protect those data?

What are the other typical ways people do that compromise security of personal data? How to avoid compromising such security?

Should NGOs formulate internal policies and provide training to staff members?

General principles under PDPO

- PDPO = Personal Data (Privacy) Ordinance (Cap. 486)
  - "**Personal Data**" means any data (a) relating to a living individual, (b) from which it is practicable to identify that individual, and (c) in a form in which access to or processing of the data is practicable.
  - "**Data User**" is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data.
- Six data protection principles ("**DPPs**") in PDPO



General principles under PDPO

- DPP 1 (purpose and manner of collection)
  - Personal data shall only be collected for a **lawful purpose directly related** to a function or activity of the data user.
  - The data collected should be **necessary** and **adequate** but **not excessive** for such purpose.
  - The **means** of collection should be **lawful and fair**.
  - The data subject is informed of the **purpose** of use of the data and classes of persons to whom the data may be transferred.

General principles under PDPO

- DPP 2 (accuracy and duration of retention of personal data)
  - All **practicable steps** shall be taken to ensure that:
    - personal data is **accurate** having regard to the purpose for which the data is to be used.
    - personal data is **not kept longer than is necessary** for the fulfillment of the purpose for which the data is to be used.

General principles under PDPO

- DPP 3 (use of personal data)
  - Personal data shall not be used for a new purpose without **consent** of the data subject.
  - If the data subject is a **minor** and is incapable of understanding the new purpose, a person who has parental responsibility for the minor may give consent for using his/her personal data for a new purpose; the use of such data for new purpose should be **clearly in the interest** of the data subject.

General principles under PDPO

- DPP 4 (security of personal data)
  - All **practicable steps** shall be taken to ensure that any personal data held by a data user is protected against **unauthorized or accidental access, processing, erasure, loss or use** having particular regard to –
    - the kind of data and the harm that could result if any of those things should occur;
    - the physical location where the data is stored;
    - any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
    - any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
    - any measures taken for ensuring the secure transmission of the data

General principles under PDPO

- DPP 5 (information to be generally available)
  - All **practicable steps** shall be taken to ensure that a person can –
    - ascertain a data user's **policies and practices** in relation to personal data;
    - be **informed** of the **kind** of personal data held by a data user; and
    - be **informed** of the **main purposes** for which personal data held by a data user is or is to be used.

General principles under PDPO

- DPP 6 (access to personal data)
  - A data subject shall be entitled to:
    - ascertain whether a data user holds personal data of which he is the data subject;
    - request access to personal data (i) within a reasonable time; (ii) at a fee (if any) that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is intelligible;
    - request correction of personal data;
    - be given reasons if such request for access/correction is refused; and
    - object to the above refusal.

General principles under PDPO

- General principle:
  - Regardless of whether one works in the office or works from home, the same standard should apply to the security of personal data and the protection of personal data privacy.

WFH Arrangements

Can NGO staff members carry materials (hard copies or electronic data through laptops etc.) containing personal data back to their home?

- As far as practicable, NGO staff members should not carry materials out of office premises, in particular for those documents containing personal data or restricted information.

WFH Arrangements

What if it is necessary to bring such materials home? What can staff members do to better protect those data?

- If it is necessary for employees to bring paper documents home for work, consider taking the following steps:
  - **Seek approval from supervisors**;
  - **Redact or remove personal data** before leaving office, where practicable;
  - Keep a **register** of paper documents that have been taken home;
  - Take **extra care** of the paper documents when travelling;
  - Lock paper documents in a **secure cabinet** or drawer at home to prevent unauthorised access;
  - Return the paper documents to offices ASAP when they are no longer necessary; and
  - No disposal at home – should be **shredded** in accordance with established procedures in the office.

WFH Arrangements

What are the other typical ways people do that compromise security of personal data? How to avoid compromising such security?

1. Remote access to corporate network using personal devices
2. Work in public places
3. Use of unsecured network in accessing corporate network
4. Use personal email accounts or instant messaging applications to send and receive companies' data
5. Use of video conferencing

Issue 1: Remote access to corporate network using personal devices

- Recommended practice for Organisations:
  - Provide employees with corporate electronic devices
  - Pre-vet and authorize employees' personal devices
  - Take technical steps to ensure data and device security
- Recommended practice for Employees:
  - Use only corporate electronic devices for work
  - Take technical steps to ensure data and device security

Issue 2: Work in public places

- Recommended practice for Employees:
  - Avoid working in public places to prevent accidental disclosure of personal data
  - Use screen filters to protect information displayed
  - Do not use public Wi-Fi

Issue 3: Use of unsecured network in accessing corporate network

- Recommended practice for Organisations:
  - Consider using VPN to connect to corporate network
  - Grant access rights to employees on a need-to-access basis
  - Enable account lockout function to prevent login by a user after multiple failed login attempts
  - Review logs of remote access to identify any suspicious activities
- Recommended practice for Employees:
  - Opt for wired connection where possible
  - Take technical steps to enhance security of connection if Wi-Fi is used

Issue 4: Use personal email accounts / instant messaging applications to send and receive companies' data

- Recommended practice for Employees:
  - Avoid using personal email accounts or instant messaging applications for work
  - Use only corporate email accounts for sending and receiving work-related docs and info
  - Double check recipient names before sending emails and instant messages
  - Beware of phishing and malicious emails and do not open suspicious links or attachments
  - Verify genuineness of suspicious emails and messages with the senders by other channels

Issue 5: Use of video conferencing

- Recommended practice for Organisations:
  - Select appropriate video conferencing software
  - Take IT security measures when using video conferencing software
  - If being a host, consider taking the following steps:
    - Set up a unique meeting ID and a strong and unique password for conference
    - Provide the meeting ID and the passwords to the intended participants only
    - Arrange one more “host” to deal with administrative, technical and other contingent issues during conference
    - Set up a virtual waiting room and validate participants’ identities before joining conference
    - “Lock" the meeting when all participants have been admitted
    - Only allow those participants who need to make presentations to share their screens or documents
    - Inform all participants and obtain their consents before recording the conference; prohibit participants from recording the conference
    - Store the records of the conference securely and delete the records when they are no longer necessary

Issue 5: Use of video conferencing

- Recommended practice for Participants:
  - Use virtual backgrounds if necessary
  - Turn off microphones (and/or cameras) when not speaking
  - Avoid discussing personal or sensitive information as far as practicable
  - Close unnecessary documents and windows before sharing screen

WFH Arrangements

Should NGOs formulate internal policies and provide training to staff members?

- Develop comprehensive privacy management programme to employees
- Develop information security guidelines and policies

WFH Arrangements

- Sample of privacy management programme manual for NGOs: https://www.pilnet.org/resource/privacy-management-programme-manual/

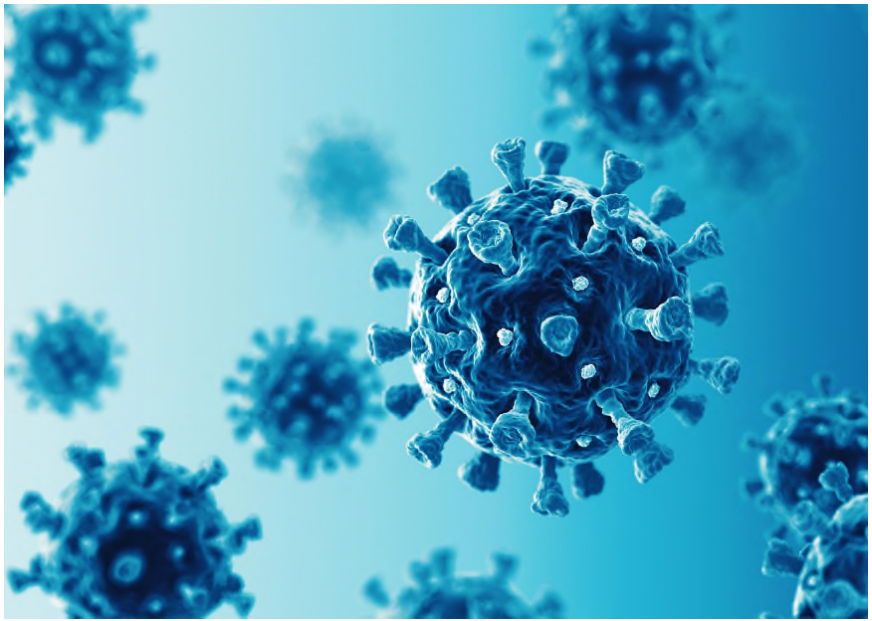
WFH Arrangements

- Provide training to staff members
- Possible topics / areas:
  - Privacy regulations and WFH arrangements
  - Data security techniques and awareness
  - Awareness about cybersecurity threats and trends

2. Vaccine Pass Requirements

Morgan Lewis

Vaccine Pass Requirements



- Should NGOs require visitors to scan "Leave Home Safe", check Vaccination and Testing Record, and check temperature before their entry?
- Are these records considered "personal data" under the PDPO? If so, will the NGOs be considered to be collecting / processing / storing "personal data"?
- Is there anything NGOs should be mindful of for the purpose of compliance with the PDPO?

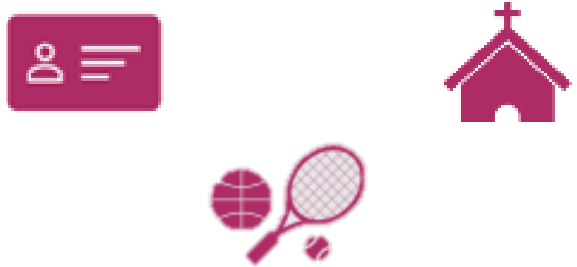
Vaccine Pass Requirements

Should NGOs require visitors to scan "Leave Home Safe" and Electronic Vaccination and Testing Record, and check temperature before their entry?

- Prevention and Control of Disease (Requirements and Directions) (Business and Premises) Regulation (Cap. 599F)
- Subject to certain exceptions, for all **Scheduled Premises**, visitors are required to
    i. scan the "Leave Home Safe" venue QR code;
    ii. conduct body temperature screening; and
    iii. comply with the requirements applicable to persons entering or remaining on the relevant premises in the Vaccine Pass Direction (*updated from time to time)

Vaccine Pass Requirements

- Examples of Scheduled Premises
  - **Event Premises**
  - Premises that are maintained or intended to be maintained for hire for holding social gatherings (e.g., party rooms)
  - Club-house
  - Sports premises
  - Religious premises
  - Market



Vaccine Pass Requirements

- Event premises:
  - Premises that (a) are **not private premises or a place of public entertainment**; and (b) are for the time being used for holding a **specified event**
  - "Specified event" means an event that the organizer adopts access control measures; with the attendees being the organizer, person who provides services, and person with invitation/prior acceptance/permit, or as representative of a body or organisation specifically invited
  - Examples of "specified event": meeting, forum, symposium, exhibition, ceremonial event and celebratory event

Vaccine Pass Requirements

- Who is currently not required to use the "Leave Home Safe" mobile application?
  - persons aged 65 or above or aged 15 or below
  - persons with disability
  - other persons recognized by the Government or organisation(s) authorized by the Government as eligible for the above arrangement
- If a person belonging to the above 3 categories is unable to use the "Leave Home Safe" mobile application, he/she should use a specified form to register his/her visit records, the premises operator must keep the written or electronic records for 31 days.
- For those aged 15 or below who is unable to use the app, if the adult accompanying him/her has used the app to scan the venue QR code or used a specified form to register relevant information, he/she would not have to register his/her information using any specified form.
- See next slide for a sample of "specified form".

Specified Declaration / Information Collection Form for Persons in relation to the "Vaccine Pass" and "LeaveHomeSafe" requirements

[The completed form is to be kept on the premises by the person-in-charge of the premises for 31 days for checking.]

Applicable to the following patrons:

(1) Holding a vaccination record of having received COVID-19 vaccine(s) outside Hong Kong[1], without a relevant QR code issued in Hong Kong; or
(2) Children aged below 12 not accompanied by an adult; or
(3) Specified person not required to use "LeaveHomeSafe" mobile application before entering the premises.

Purposes of collecting personal data:

The information provided by you will only be used to facilitate the work of the Government in controlling the spread of COVID-19 and for related purposes. Only persons authorised by this premises will have access to such information for the aforesaid purposes. For the purposes of epidemiological investigation, contact tracing, and investigation and prosecution in relation to breaches of the relevant legislation, where necessary, the information supplied by you may be provided to the Government/other organisations/associations/persons, such as the Department of Health (including the Centre for Health Protection), the Hospital Authority and authorised law enforcement officers. If you wish to amend or access the personal information provided, please contact Mr/Ms at . It is the premises' right to deny your entry should you fail to provide the required personal information.

I am fully aware of the relevant directions made by SFH under the Prevention and Control of Disease (Vaccine Pass) Regulation (Cap. 599L) in respect of the "Vaccine Pass" and the Prevention and Control of Disease (Requirements and Directions) (Business and Premises) Regulation (Cap. 599F) in respect of the "LeaveHomeSafe" requirements, and confirm to the person-in-charge of the premises that I am –

☐ **Regarding the "Vaccine Pass" requirement (please tick "✓" if applicable)**

- ○ **holding a vaccination record of having received COVID-19 vaccine(s) outside Hong Kong, without a relevant QR code issued in Hong Kong.** I have received the first dose of COVID-19 vaccine in_____ (name of country / place), the second dose* of COVID-19 vaccine in_____ (name of country / place), and the third dose* of COVID-19 vaccine in_____ (name of country / place) as stipulated in the guidelines issued by the local health authority. I undertake to keep the aforesaid vaccination record for checking.
- ○ **a child aged below 12 not accompanied by an adult**

☐ **Regarding the "LeaveHomeSafe" requirement (please tick "✓" if applicable)**
(i) aged 15 or below and not accompanied by an adult or aged 65 or above; or (ii) a person with disability; or (iii) other persons recognized by the Government or organization(s) authorized by the Government as eligible for the above-mentioned alternative arrangement.

* delete as appropriate

[1] Receiving COVID-19 vaccines outside Hong Kong means having received in places outside Hong Kong of the relevant COVID-19 vaccine, subject to the vaccine used being included on the list of vaccines recognised for this purpose as published on the Government's COVID-19 Thematic Website. (https://www.coronavirus.gov.hk/pdf/list_of_recognised_covid19_vaccines.pdf)

Particulars required to be filled in by patron

Name:	
Telephone number:	
Date of visit:	
Time of visit:	

Signature: _____ Date: _____

有關「疫苗通行證」及「安心出行」規定的顧客申報／提供資料指定表格

[此表格填妥後須由處所掌管人保存在處所內 31 天以供查核]

以下顧客適用：
(1) 出示香港以外地區接種新冠疫苗紀錄(而沒有相關在香港發出的二維碼)[1]；或
(2) 12歲以下沒有成人陪同的兒童；或
(3) 未能在進入處所前使用「安心出行」流動應用程式的指定人士

收集個人資料的目的：

你提供的資料只供協助政府應對 2019 冠狀病毒病蔓延的工作及相關的用途，本處所授權人員基於上述目的方可查閱。為流行病學調查和接觸追蹤工作以及進行違反相關法律的調查及檢控工作的目的，你提供的資料在有需要時，可提供予政府／機構／組織／人士，例如衞生署（包括衞生防護中心）、醫院管理局及獲授權的執法人員等。如你欲更改或查閱所申報的個人資料，請與【　　先生/女士】聯絡(電話:　　)。如你未能提供所需的個人資料，本處所有權拒絕你進入處所。

本人清楚知悉食物及衞生局局長根據《預防及控制疾病(疫苗通行證)規例》(第599L章) 就「疫苗通行證」及《預防及控制疾病(規定及指示)(業務及處所)規例》(第599F章) 就「安心出行」規定發出的相關指示，並向處所掌管人確認本人：

☐ **關於「疫苗通行證」規定** (如適用請填上「✓」號)

- ○ **出示香港以外地區接種新冠疫苗紀錄(而沒有相關在香港發出的二維碼)。**按當地衞生當局的指引，本人是在_____(國家／地方名稱)接種第一劑*；在_____(國家／地方名稱)接種第二劑*；及在_____(國家／地方名稱)接種第三劑*新冠疫苗。本人承諾會保存上述接種紀錄，以供查核。
- ○ **為12歲以下沒有成人陪同的兒童**

☐ **關於「安心出行」規定** (如適用請填上「✓」號)
為(i) 15歲或以下並沒有成年人士陪同，或65歲或以上；或(ii) 殘疾人士；或(iii) 其他就上述替代安排獲政府或政府授權機構認可為合資格的人士。

*刪去不適用者

[1] 在香港以外地方接種了新冠疫苗而該疫苗載列於政府 2019 冠狀病毒病專題網站的名單上：(https://www.coronavirus.gov.hk/pdf/list_of_recognised_covid19_vaccines.pdf)

顧客須填寫資料

姓名：	
聯絡電話：	
到訪處所日期：	
到訪處所時間：	

簽名：_____ 日期：_____

Vaccine Pass Requirements

- Vaccine Pass Direction issued under the Prevention and Control of Disease (Vaccine Pass) Regulation (Cap. 599L)
  - Subject to certain limited exceptions, a person shall not enter or remain on any **Specified Premises** unless the person has been vaccinated in the specified manner for the purposes of a Vaccine Pass Direction
  - The Specified Premises and Scheduled Premises are similar, both including Event premises
- Certain types of Specified Premises require the person in charge's active checking of the vaccine pass of visitors

Vaccine Pass Requirements

- Liability for non-compliance
  - Persons in charge: A maximum fine of $50,000 and imprisonment for 6 months
  - Visitors: A maximum fine of $10,000

Vaccine Pass Requirements

Are these records considered "personal data" under the PDPO? Will the NGOs be considered to be collecting / processing / storing "personal data"?

General Principle:

A visitor's name, address, contact details, health conditions are all personal data. Body temperature data and location data *per se* are not regarded as "personal data". However, they may be viewed together with other personal data such as the name, facial image and contact details, which may directly or indirectly identify an individual.

The PCPD has opined that the "Leave Home Safe" App and Vaccine Pass are in compliance with the requirements of the PDPO.

Vaccine Pass Requirements

- Rationale:
  - When a visitor scans the venue's Leave Home Safe QR code, no personal data would be displayed
  - The app **will not use the GPS function or other data in the mobile phone** and therefore users' whereabouts will not be disclosed to others.
  - Visit records originating from the visitors' vaccination records and containing personal data, would be **masked and hashed**, resulting in the production of **unidentifiable data** stored in the mobile device of the venue operators.
  - The visit records would be **encrypted**, making them inaccessible to the venue operators.
  - The visit records would only be temporarily saved **for 31 days for anti-epidemic purposes**, after which the date would be **deleted automatically**.

Vaccine Pass Requirements

- Rationale:
  - Users will have complete control over the vaccination and testing records kept in the app, and may choose to show the information or not to any third parties, and can remove the records from the app at any time.
  - The app will not upload the records to any computer systems including the government system.
  - Only in the event of confirmed patient having visited the premises that the health authorities would request the visit records be uploaded to the government's private cloud. The records would then be retrieved and further processed via encrypted channels by authorised personnel for epidemiological investigation, including contact tracing, thus effectively mitigating data security risks.

Vaccine Pass Requirements

Is there anything NGOs should be mindful of for the purpose of compliance with the PDPO?

- Mindful of the 6 data protection principles:
  - DPP 1 (purpose and manner of collection of personal data)
  - DPP 2 (accuracy and duration of retention of personal data)
  - DPP 3 (use of personal data)
  - DPP 4 (security of personal data)
  - DPP 5 (information to be generally available)
  - DPP 6 (access to personal data)

Vaccine Pass Requirements

- Exemptions to the application of DPPs in the anti-pandemic context
  - If the use of the data is required or authorized by any enactment, rule of law or an order of a court in Hong Kong, DPP3 can be exempted
  - For example, in suitable cases, an organizer of event may be required to provide personal information of certain visitor without obtaining prior consent from the visitor in relation to the disclosure.
  - Cap. 599L provides an authorized officer with the power to require any person to provide any information to facilitate him discharging his function in suitable cases

Vaccine Pass Requirements

- Ensure that the sole purpose for using the personal data of the data subject is to help protect the public health
- The privacy of the data subject should be respected at the same time
- The data user is advised to seek assistance from the relevant medical staff or the Food and Health Department to ensure that the use of the personal data does not exceed the permissible scope

Vaccine Pass Requirements

In an employment context under Covid-19

- It is generally justifiable and reasonable for employers to collect temperature measurements, travel histories, vaccination records, COVID-19 test results, infection records from the employees
- Employer's responsibility to assess the risk of transmission of the coronavirus in the workplace and safeguard the health of employees and visitors
- Employers should only collect health data that is necessary for or directly related to the purpose of prevention or control of COVID-19 in the workplace


3. Surveillance Measures
Morgan Lewis

Surveillance Measures

- Can NGOs install surveillance cameras around their premises? Any practical tips to ensure compliance with the PDPO?
- Can NGOs watch / replay the recorded videos for the purpose of e.g., improving quality of work / evaluation of employees / detection of malpractices etc.? What are the limitations / boundaries the NGOs should watch out for?
- Are NGOs obliged to provide those video records to criminal enforcement agencies upon request for their investigation of crime? What are the general Do's and Don'ts for the NGOs?
- Any special points to note regarding children's personal data?

Surveillance Measures

Can NGOs install surveillance cameras around their premises? Any practical tips to ensure compliance with the PDPO?

- No legal prohibition
- Tip: ensure compliance with data protection principles
- Tip: consider purpose of collection, method of collection (any alternative methods) and use of the data collected

Surveillance Measures

Recommended best practices – the "3A" guidance

- Assessment of risks
- Alternatives to address such risks
- Accountability of the data user

Surveillance Measures

Assessment of the risks

- what is the purpose of the monitoring?
- what are the risks that the monitoring intends to manage/mitigate?
- what are the benefits of the monitoring?
- assess the existence and extent of these risks in a realistic manner
- assess the likely adverse impact on the employees
- consult the employees and document the views expressed and the evaluation process
- the surveillance measures should be necessary to meet its business purposes/the risks identified, the personal data collected are kept to a minimum necessary and the surveillance measure is carried out by the least intrusive manner.

Surveillance Measures

Alternatives to address such risks

- are there other pragmatic alternatives?
- is the surveillance confined to high-risk areas?
- surveillance during certain periods of time vs universal and perpetual basis?
- conduct the surveillance in an overt manner
- covert monitoring should not be adopted unless it is justified by special circumstances (e.g. involving reasonable suspicion of unlawful activity, detection of the unlawful activity and successful gathering of evidence)

Surveillance Measures

Accountability of the data user

Appraisal checks

- "Data User" includes employees in charge of handling personal data in the course of conducting employee monitoring

Written privacy policy

- notify your employees before monitoring is introduced
- review the policy regularly to ensure it is up-to-date and remains relevant to organisational needs

Surveillance Measures

Accountability of the data user

Retention period

- Duration?
- Routine erasure based on a predetermined schedule
- Cater for different retention period based on needs

Engagement of third party data processors

- ensure compliance with the PDPO by contract
- Tip: include right to conduct routine inspection, set out minimum security measures and standards to be adopted by data processor, abnormalities reporting requirements, measures in the event of data security issues or leakage

Surveillance Measures

PDPO implications

- The employee monitoring practices may be subject to investigation by the Privacy Commissioner in an alleged breach of the PDPO
- Be ready to explain and demonstrate that:
  1. the monitoring is only carried out to the extent necessary
  2. the personal data collected was kept to an absolute minimum and by means that are fair in the circumstances
  3. the written privacy policy has been implemented and practical steps have been taken to communicate that policy to the employees/data subjects

Surveillance Measures

- If the CCTV monitoring is in operation in locations accessible to the general public, an appropriate signage should be prominently displayed in the proximity of the CCTV cameras
  - E.g. "This area is under video monitoring for the purposes of ensuring your security and safety when visiting our premises."
- Consider and conduct the "3A" test

Surveillance Measures

Can NGOs watch or replay the recorded videos for the purpose of e.g., improving quality of work / evaluation of employees / detection of malpractices etc.? What are the limitations and boundaries the NGOs should watch out for?

- Use the data collected for purposes stated in the written privacy policy
- Practical tips:
  - Implement security and access control measures to safeguard against unauthorized and accidental access or wrongful use
  - Control access by authorized personnel only
  - Videos to be kept generally for not more than 6 months
  - redact / anonymize the features that would identify a particular employee if the records are used for training purposes

Surveillance Measures

Are NGOs obliged to provide those video records to criminal enforcement agencies upon request for their investigation of crime? What are the general Do's and Don'ts for the NGOs?

- General duty to cooperate and assist
- Ensure privacy policy includes provision of personal data to law enforcement agencies
- Exemption under section 58 of the PDPO to seek information for prevention and detection of crime

Surveillance Measures

When law enforcement agencies seek cooperation and information, consider taking the following steps:

- Review the scope of the request under the warrant / letter of request together with the CCTV footage
- Analyse the matter objectively; make an informed decision whether and what information to disclose; keep proper records of the decision-making process
- Seek clarification if the request or subject of investigation is unclear or too broad
- Disclosure on a need-to-know basis and only information that is directly relevant to the investigation
- Seek legal advice as appropriate

Surveillance Measures

Any special points to note regarding children's personal data?

- Children
  - Vulnerable group who have special requirements in privacy protection
    - More inclined to follow instructions without questioning
    - Less privacy-aware
    - Less able to exercise caution
- General Principle: Limit the collection of personal data of children
  - Involve parents, legal guardian when an organisation intends to collect children's personal data
  - Consent of, notification should be obtained from a person who has parental responsibility for the minor

4. Collection of HKID Card Information

Morgan Lewis

Key Questions on the Collection of HKID Card Information

- When is it permissible to collect HKID Card number?
- When is it permissible to collect HKID Card copy?
- Tips to facilitate compliance with PDPO?

General principles under PDPO

- DPP 1 (purpose and manner of collection)
- The Code of Practice on the Identity Card Number and Other Personal Identifiers

Basic Position

- **No right to compel** an individual to provide a HKID Card number / copy of HKID Card **unless authorised by law**
- Wherever practicable, consider **less privacy-intrusive alternatives**
  - Use other personal identifiers (e.g., employee number)
  - Accept identification of the individual by someone known to the data user
  - Accept some form of security (e.g., money deposit)

When is it permissible to collect HKID Card number?

- Some examples:
  - Empower under the law to require an individual to provide HKID Card number
  - Comply with a requirement under the law
  - For certain public or social interests
  - For identifying individual where he/she enters premises or is given the use of equipment, where monitoring of the activities of such individual is not reasonably practicable
  - As a condition for giving an individual control or custody of property which is of a value that is more than trivial
  - Generally, collection of a HKID Card number of a member by an organisation may be justified to enable the organisation to check membership (but not collecting HKID card copy for this purpose)

When is it permissible to collect copies of HKID Card?

- Some examples:
  - For certain public or social interests
  - As proof of compliance with any statutory requirement
  - Comply with a requirement endorsed by the Privacy Commissioner and is contained in the codes, rules, regulations or guidelines of a regulatory or professional body
  - Collect HKID Card copy for the purpose of collecting or checking the HKID Card number of an individual but only if the individual has been given the choice of showing his HKID Card in person

When is it permissible to collect copies of HKID Card?

- Specific circumstances **NOT sufficient** to justify the collection of a HKID Card copy:
  - solely to safeguard against mistakes in recording the holder's name or HKID Card number
  - solely in anticipation of a possible relationship between an individual and the organisation

Tips to facilitate compliance with PDPO

- DPP 2 (accuracy and duration of retention of personal data)
- Consider taking one or more of the following steps to ensure accuracy:
  - Collect directly from the HKID Card physically produced
  - If provided without showing HKID Card (e.g., by post / phone), check against physical production of HKID Card in person before using the number for any purpose
  - If given the option to provide a copy of the HKID Card or to present the HKID Card in person, and he/she has chosen the former, the data user may be permitted to collect the HKID Card number from such a copy

Tips to facilitate compliance with PDPO

- How about HKID Card copy (assuming allowed to collect)?
  - Always **check against the HKID Card**
  - Ensure third party has checked the copy against the HKID Card concerned when the copy is collected from a third party
  - NGO may also consider taking the following steps:
    - Give **training** to staff to enable them to detect irregularities on the face of HKID Card copies
    - **Retain record** and indicate if the copies have been collected without being checked against the HKID Cards concerned

Tips to facilitate compliance with PDPO

- DPP 2 (accuracy and duration of retention of personal data)
  - All **practicable steps** must be taken to ensure that personal data is **not kept longer than is necessary** for the fulfillment of the purpose for which the data is to be used.

Tips to facilitate compliance with PDPO

- DPP 3 (use of personal data)
- Use of HKID Card number / copy
  - Use only for the purposes allowed under the Code of Practice (see above)
  - A purpose to which the individual has voluntarily given **express consent**
  - A purpose permitted by an applicable exemption in the PDPO

Tips to facilitate compliance with PDPO

Security safeguard measures

- DPP 4 (security of personal data)
- HKID Card number
  - Unless required or permitted by law, a data user should not:
    - publicly display together with an individual's name and HKID Card number
    - make an individual's name and HKID Card number visible together to anyone who does not need to carry out activities related to the permitted uses of the HKID Card number
    - issue a card to an individual that has the individual's HKID Card number printed on it in a legible form

Tips to facilitate compliance with PDPO

Security safeguard measures

- HKID Card copy
  - Mark "copy" across the entire image of the HKID Card in the presence of the holder
  - Treat as confidential
  - Take all reasonably practicable steps before transmitting a copy or image of a HKID Card to ensure that it is received only by the intended recipient

Presenters

Yan Zeng
Partner, Corporate and Business Transactions

yan.zeng@morganlewis.com

Justina Lam
Managing Associate, Litigation

justina.lam@morganlewis.com

Chris Kung
Managing Associate, Corporate and Business Transactions

chris.kung@morganlewis.com

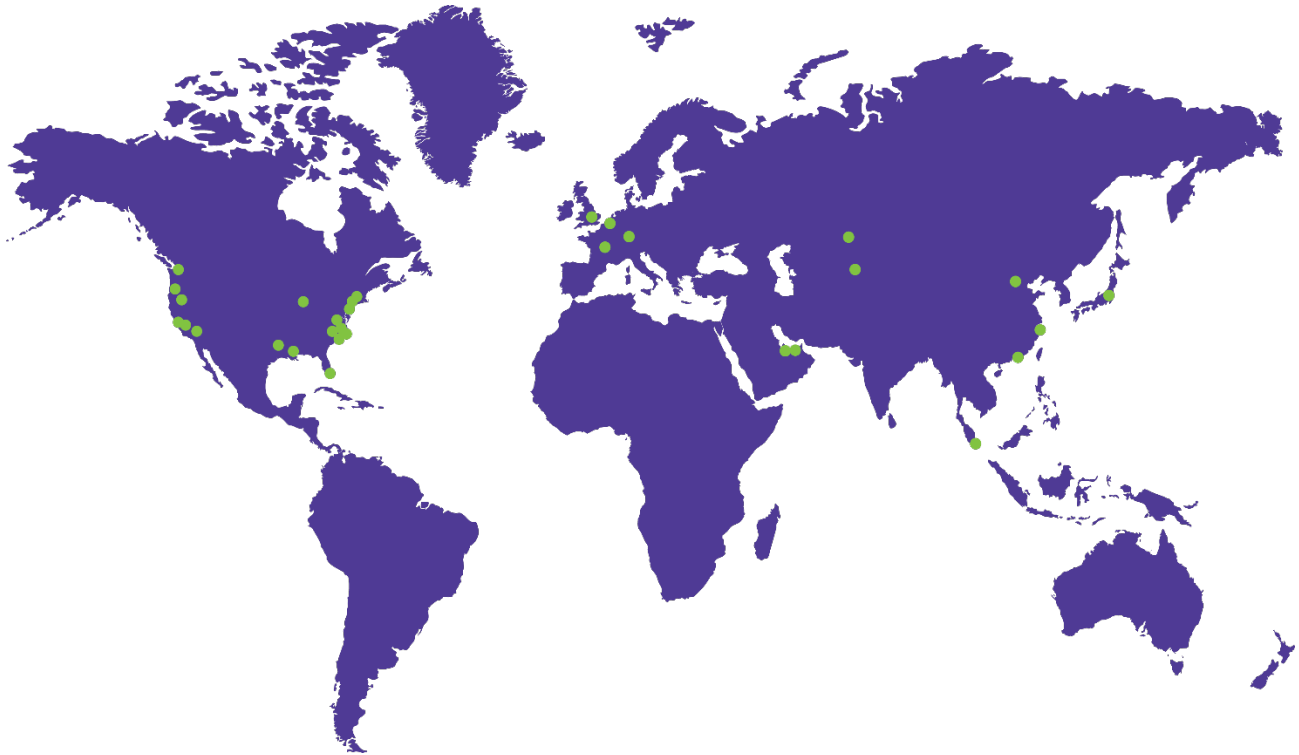
Morgan Lewis

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU