DATA PROTECTION: A PRACTICAL GUIDE

BDO

CONTENTS

1 Introduction to the Personal Data (Privacy) Ordinance

The Personal Data (Privacy) Ordinance (Cap. 486 of the laws of Hong Kong) (the Ordinance) took effect in 1996. Contraventions of certain provisions under the Ordinance may constitute criminal offences, and offenders may be liable for a maximum fine of $1,000,000 and imprisonment for up to five years upon conviction.

Key terms used in this Guidance

Personal data	Any data: • relating to a living individual; • from which the identity of the individual can be ascertained; and • in a form in which access to or processing of the data is practicable (in other words, personal data must be in a record format, e.g. written on a document or stored in a computer file). (Example: a customer's name and address stored in a paper file or an electronic file)
Data subject	An individual person who is the subject of the data. (Example: a customer who provided personal data to your company.)
Data user	A person or company that collects, holds, processes or uses the relevant personal data.
Data processor	A person or company that processes personal data on behalf of another person or company (a data user) rather than for his/its own purposes. (Example: An external service provider that your company has appointed to help conduct a customer survey by collecting customer data and delivering that data and the survey results to your company.)

The Ordinance and the Office of the Privacy Commissioner for Personal Data

The Ordinance aims to protect the personal data of a data subject by regulating any data user that collects, holds or uses personal data, and by preventing and penalising any abuse or negligence in handling personal data by data users in Hong Kong.

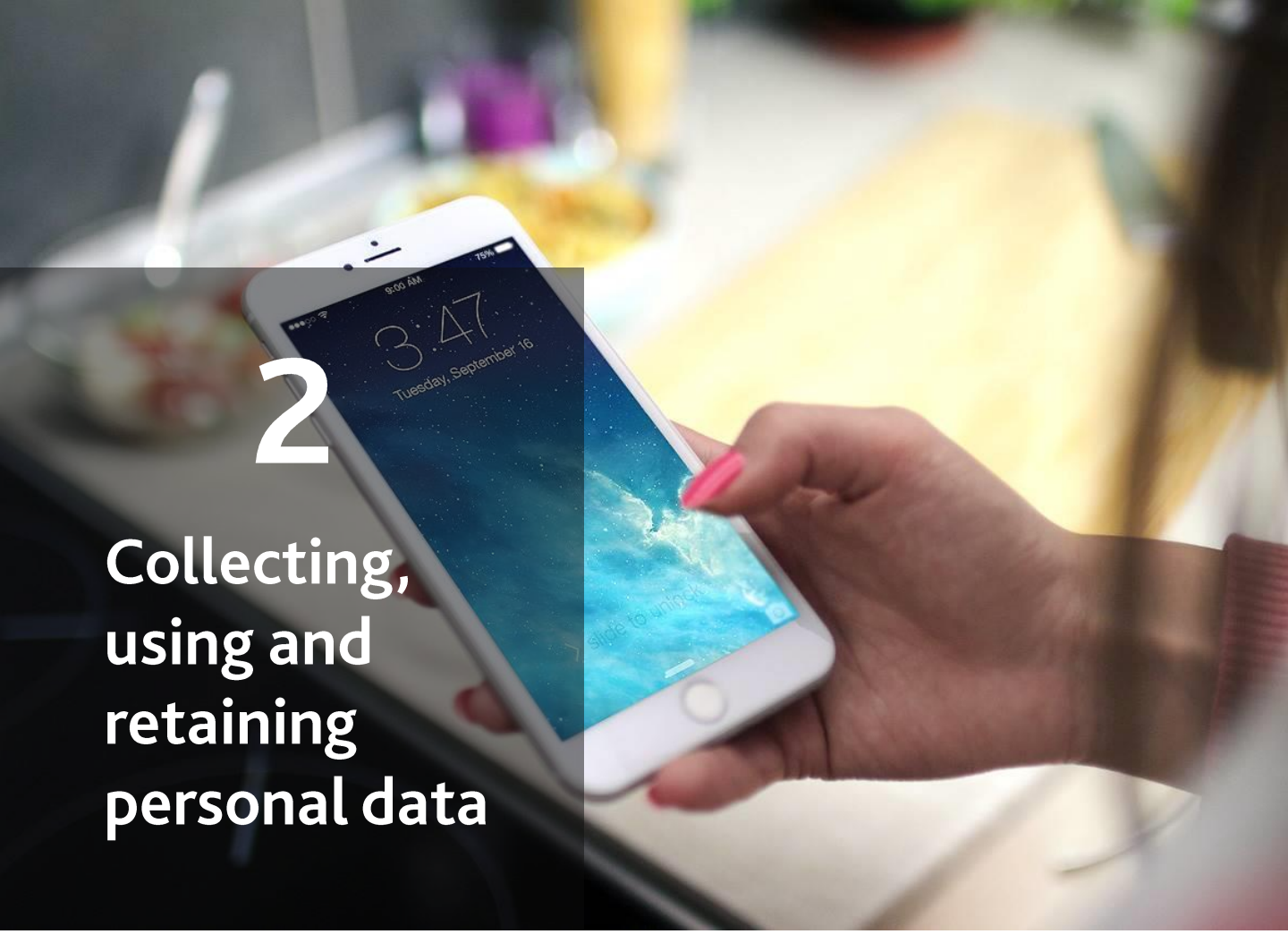
The gist of the Ordinance is contained in its six Data Protection Principles (DPPs). More information about the DPPs is provided in Appendix 1, and examples of some criminal offences imposed by the Ordinance are listed in Appendix 2.

As well as leading to fines and imprisonment, violating the Ordinance may attract public attention and cause substantial damage to the reputation of the data user. In addition, the aggrieved data subject (e.g. the affected customer) may launch a civil lawsuit against the relevant data user to claim compensation.

The Office of the Privacy Commissioner for Personal Data (PCPD) was established under the Ordinance as the data privacy regulator in Hong Kong. It monitors data users in the public and private sectors for compliance with the provisions of the Ordinance. The PCPD investigates complaints from the general public about breaches of the Ordinance, and issues codes of practice and guidelines to help data users learn more about the requirements of the Ordinance.

Foreign data privacy laws

In addition to the Ordinance, overseas data privacy laws may apply to companies that are involved in collecting and processing personal data from foreign countries. A prominent example is the European Union (EU) General Data Protection Regulation (GDPR), which took effect on 25 May 2018. The GDPR has extra-territorial application to non-EU companies that perform data processing activities related to people who are located in EU member states. For more information about the GDPR, see Appendix 3.



2 Collecting, using and retaining personal data

A. Collecting and using personal data

You should ensure that personal data is collected properly in line with the following guidance:

i. Only collect personal data for lawful purposes that are directly related to your company's business purpose or activities.

ii. Only collect the personal data which is necessary for or directly related to that purpose, and never collect more data than you need for that purpose.

iii. Do not use illegal or misleading methods to collect personal data.

iv. On or before collecting personal data, give the data subject information about:

- the purpose for which the data will be used;
- the classes of persons to whom the data may be transferred (including third party service providers, if applicable);
- the consequences if he fails to supply the data (e.g. he will not be able to purchase or use certain products or services); and
- his rights to request access to and correction of his personal data held by your company (and information about how to contact you).

Before you collect personal data from a data subject (a customer or an employee), consider providing him with a personal information collection statement (PICS) containing all the information set out in (iv) above.

Use of personal data must be limited to the purposes as you had notified at the time of data collection, unless you have obtained consent from the relevant data subjects to use their data for a new purpose. You should also carefully consider the types of information that you need to collect from the data subject to fulfil your business purpose. For example, if you expect future communication with your customer to be by phone or email, you should not collect the customer's postal address.

Do not collect Hong Kong Identity Card numbers (or copies of these ID cards) from customers or anyone else unless you need them for a human resources purpose (e.g. recruitment or employment), for complying with a data access or data correction request, or for complying with statutory requirements.

Direct marketing

Before collecting personal data from existing or potential customers for direct marketing activities (e.g. sending promotional letters or emails), you must:

i. inform the customers that your company wants to use their personal data for direct marketing and what you will be promoting (e.g. the products, services or events offered by your company);

ii. inform the customers about the types of personal data you want to use;

iii. provide the customers with a response channel through which they can communicate their consent in writing to your company (e.g. by adding an independent section to a registration form where new members can give your company consent to use their personal data for direct marketing);

iv. obtain the customers' written consent before you use their personal data for direct marketing; and

v. obtain specific consent from the customers if you also want to provide their personal data to another company for use by that company for directing marketing.

You can include the information referred to in items (i), (ii), (iii) & (v) in the relevant PICS, application form or registration form.

Opting out of direct marketing communications

Employees and departments involved in sending direct marketing communications and/or handling opt-out requests must maintain and update lists of customers who have opted in and customers who have opted out. Both lists should be centralised, so all departments that may send direct marketing messages can access them.

All direct marketing communications must contain a statement informing recipients that they can opt out of, or unsubscribe from, future marketing messages from your company. The statement must also explain how to unsubscribe. After receiving an opt-out request from a customer, the handling staff must stop sending direct marketing messages to that customer and promptly update the opted-in and opted-out lists.

B. Accuracy, retention and erasure of personal data

You should take practicable steps to ensure that all personal data held by your company:

i. is accurate;

ii. is not kept longer than is necessary for the fulfillment of the purpose for which the personal data is being used (or is intended to be used); and

iii. is properly erased when the relevant retention period has expired.

It is best practice to formulate a data/document retention policy that sets out the maximum retention periods for different kinds of personal data for different operational and legal requirements.

Electronic or paper files containing obsolete or out-of-date personal data must be erased or destroyed properly. If your company has appointed an external contractor to handle this process, the contractor must be regulated by a signed service agreement that sets out their data protection obligations.

3 Data security and preventive measures

A. Privacy management programme

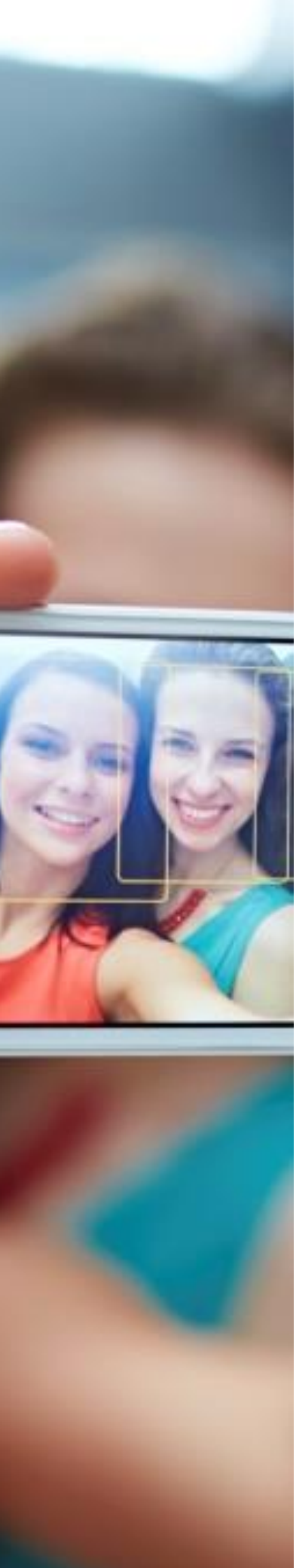
Implementing a privacy management programme (PMP) enables a company to comprehensively review its existing practices for handling personal data and set up effective data-handling guidelines and procedures that are tailored to the business nature of the whole company. A PMP can also facilitate compliance with the Ordinance in all departments by employees at all levels who may handle personal data for the company.

Here are some important tasks to include in a PMP:

i. Appointing a Data Protection Officer, who will oversee all matters relating to data privacy for the company.

ii. Nominating a data protection coordinator in each department, who will handle routine privacy matters in his department and liaise with the Data Protection Officer on matters such as reporting data breach incidents and consultation on complex data privacy issues.

iii. Reviewing the inventory of personal data, which is to check and record the types of personal data held in each department, the purposes of collecting that data, the people who can view and use the data, how the data is stored, the retention periods for the data, etc.

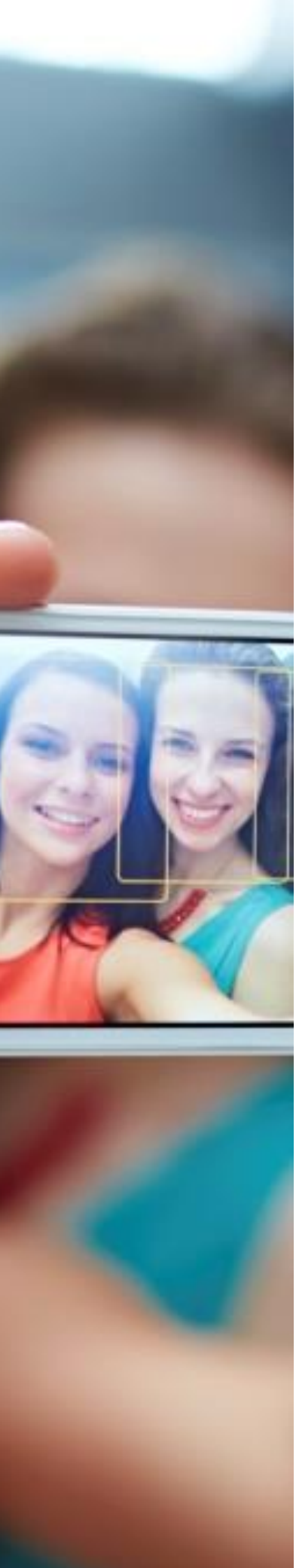


iv. Devising policies and procedures for handling personal data. Depending on the nature of your business, you may develop one comprehensive guide or different sets of policies and procedures (e.g. one for direct marketing and one for human resources management). Those policies and procedures should cover all steps in handling data: collection, use and disclosure, retention and disposal, security measures, and responding to data access requests, etc.

v. Monitoring gaps in compliance in order to: (a) review the existing data handling practice in each department and identify any loopholes with regard to the relevant data privacy regulations; (b) set out the remedial actions and implement them; and (c) regularly monitor and assess the effectiveness of the remedial actions to see if any outstanding issues need to be rectified.

vi. Setting up a system for reporting data breaches. This system should cover the procedures for escalating data breaches to senior staff and notifying the affected data subjects (for more details, see section 4).

(Reference: PCPD's Privacy Management Programme Manual (for Private Sector))



B. Privacy impact assessment

Conducting a privacy impact assessment (PIA) may help minimise data privacy risks when there is a new activity or project that involves collecting and using personal data or there is a significant change in the data-handling process for an existing activity or project.

In general, a PIA involves:

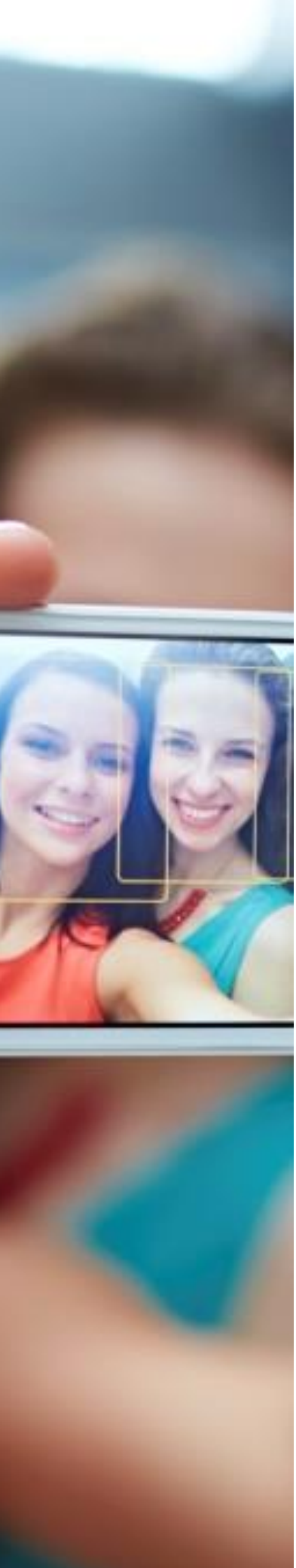
i. conducting a data processing cycle analysis;

ii. conducting a privacy risk analysis;

iii. avoiding or mitigating privacy risks; and

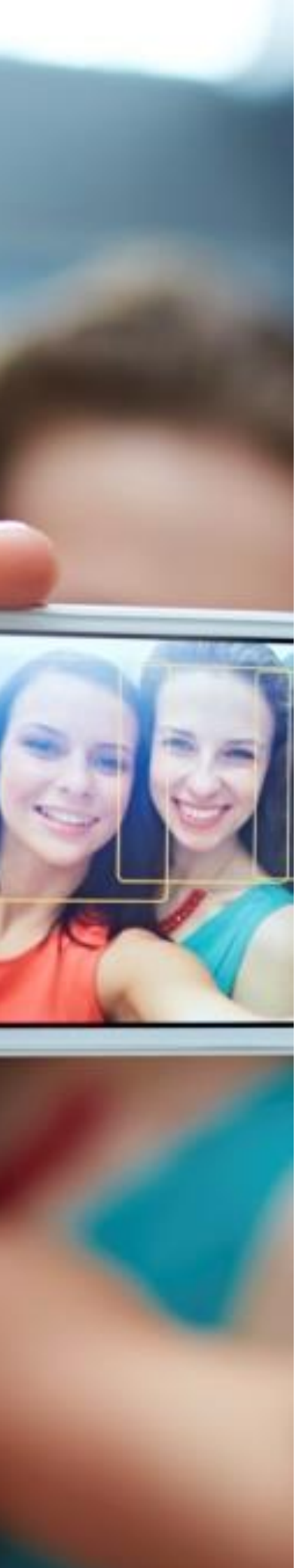
iv. reporting and continuous monitoring.

(Reference: PCPD's information leaflet on Privacy Impact Assessment)



C. Other examples of data security and preventive measures

i.	Set out clear guidance on access rights that apply to viewing and using personal data on different occasions. The general rule is that data should be accessed on a "need-to-know" basis.
ii.	Apply security measures to IT systems, computer servers and electronic data files. Here are some examples: • If you collect customers' personal data and payment details online, take practicable steps to ensure that the data transmission between the customer's device and your server is secured by, for example, using a Secure Sockets Layer (SSL). Sensitive data (such as HKID, bank account and credit card numbers) should be masked when it is stored on your server. • Protect all desktop or notebook computers provided by your company with a login ID and password set by individual employees. Those computers should automatically sign out if they are left unattended for more than 5–10 minutes. • Set up an access log to record employees' access to computer systems that store personal data about customers or staff.
iii.	Apply security measures to paper documents and files. Here are some examples: • Do not leave documents that contain personal data unattended, and store them in locked cabinets. • Ensure that employees clear their desks when they are off-duty. • Destroy obsolete documents that contain personal data by using a shredder. You may also consider appointing a reputable service provider to destroy large volumes of obsolete documents.
iv.	If you need to send files that include personal data by email, ensure that they are encrypted. Send passwords for opening the files in a separate email. Also, you must check the recipient's email address before clicking "send" or "reply" in order to avoid sending confidential information to any unintended recipients.



v.	Regulate employees' use of social media platforms. Employees should never disclose sensitive company information and employee personal data (except their own personal data) on social media. Recommend that employees enhance their privacy settings on their social media accounts (e.g. by restricting access to their accounts to designated people only).
vi.	Do not use portable data storage devices (e.g. USB flash drives) to store personal data. If you have to use such devices for business purposes, put in place the following requirements: • Employees must only use devices provided by their company, and a proper log must be used to record the date and time of borrowing. • All data files in the devices must be encrypted. • Avoid taking the devices away from the office premises.
vii.	Provide training for employees on all the preventive measures used by your company. In addition, issue regular reminders to refresh their awareness of the relevant measures.

4

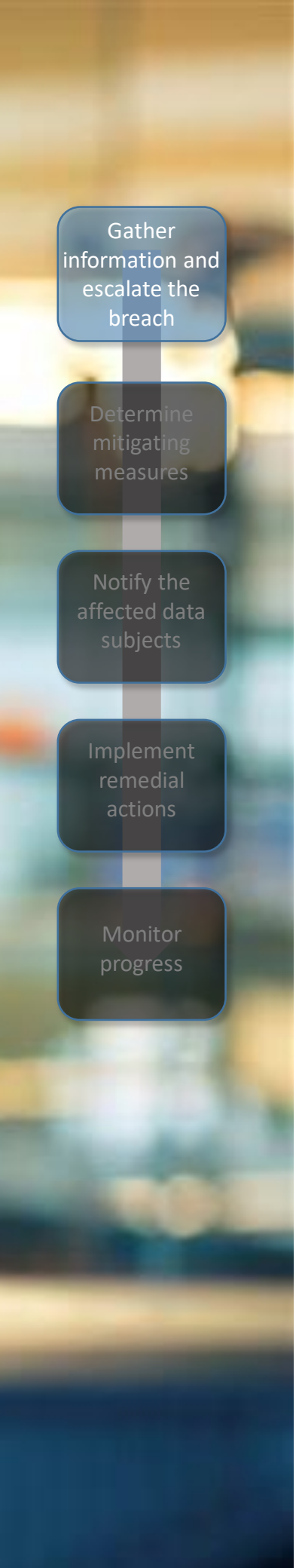
Handling data breach/data leak incidents

The Ordinance does not define the term "data breach". In general terms, a data breach is an incident that relates to accidental or unauthorised access, processing, erasure, loss, use or disclosure of personal data. Most data breach incidents are the result of inadequate data security measures, so a data user who has committed a data breach might have violated the data security requirements under DPP 4 of the Ordinance.

Examples of data breaches:

- Losing a portable storage device (e.g. a mobile phone, a USB flash drive or paper file) that contains customers' or employees' personal data.
- A computer server storing a customer database being hacked by an unknown person over the Internet.
- Improper disposal of personal files that contain copies of employees' ID cards, appraisal forms, etc.

If a data breach occurs, the relevant parties (e.g. the staff who committed the breach, the data protection coordinator of the responsible department, and the Data Protection Officer) should work through the following procedures together:



A. Gather information and escalate the breach

i. The employee who committed or discovered the data breach must immediately gather as much information as possible in answer to the following questions, and then notify his immediate supervisor.

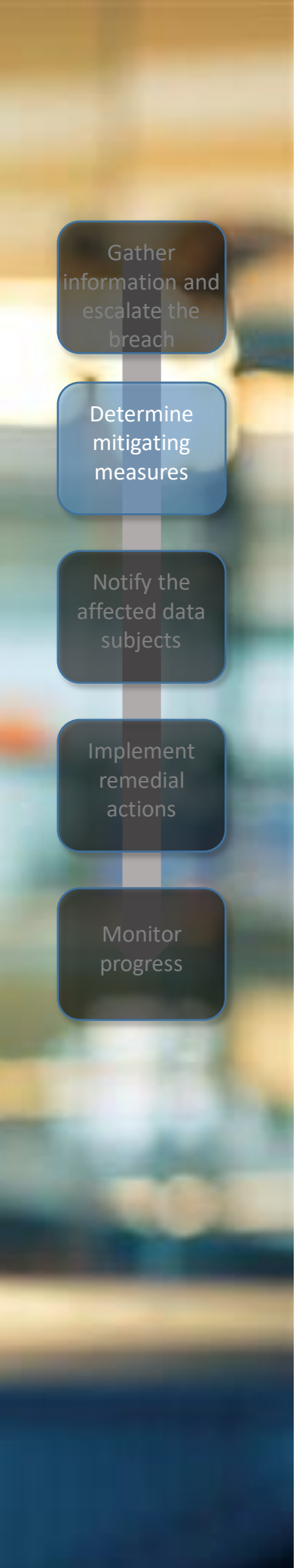
- When and where did the incident take place? For example, which customer database was hacked?
- What kinds of personal data are involved? For example, names, telephone numbers or email addresses?
- Which groups of data subjects are affected? For example, customers, members of the XXX programme or staff in the XXX department?
- How may data subjects have been affected?
- Is the data processor involved?
- What was the cause of the data breach, and how was the incident discovered?

(Note: If the responsible employee is unable to gather the above information, his immediate supervisor must help him to do so.)

ii. The responsible employee and/or his immediate supervisor must report the details of the incident to the data protection coordinator of the relevant department, who must then report those details to the head of department and the Data Protection Officer.

iii. The Data Protection Officer should then assess the seriousness of the incident (e.g. the possible level of harm resulting from the incident) to determine whether it must be reported to senior management.

When deciding whether or not to report the incident to senior management, the Data Protection Officer may consider matters such as the number of affected customers, the potential financial loss, the anticipated damage to the company's reputation and any criminal liability involved.



B. Determine mitigating measures

Depending on the circumstances of the data breach, interim actions should be taken immediately in order to mitigate the loss and limit the extent of the data breach. Here are some examples:

- If the incident relates to a computer system failure or an invasion by hackers, temporarily suspend the relevant system and consult an IT expert about closing any loopholes.
- If the incident involves an external service provider or data processor, urge that data processor to take remedial action immediately. If necessary, work with the data processor to tackle the issues together.
- If the incident involves criminal activities (e.g. an employee stealing customer data to sell), the Data Protection Officer should consider seeking legal advice and notifying the relevant law enforcement agencies.

C. Notify the affected data subjects (and the PCPD, if necessary)

Under the Ordinance, it is not mandatory for the data user to notify the affected data subjects when a data breach has occurred. However, it is a good practice to do so, as the affected data subjects can then be warned about the incident and take the necessary precautions to avoid further loss. The notification may include the following information:

- General information about the incident (e.g. when and where it happened, what kinds of personal data were involved and what the cause of the incident was).
- What sort of remedial action has been (or will be) taken.
- What sort of assistance or recommendations your company can offer the affected data subjects.

If the Data Protection Officer is of the view that the data breach is serious, the PCPD should also be notified. The PCPD has prepared a Data Breach Notification Form, which can be downloaded from its website.

Notifications may also be given to other relevant law enforcement agencies and regulatory bodies (e.g. the police or the Hong Kong Monetary Authority). Data users should seek legal advice about this, as it may be mandatory to notify particular regulatory bodies if certain types of data breaches have occurred.

D. Implement remedial actions

Further remedial actions may have to be taken in addition to the interim actions set out in procedure B. The remedial actions that are needed will depend on the circumstances of the incident. Here are some matters you should consider before taking further action:

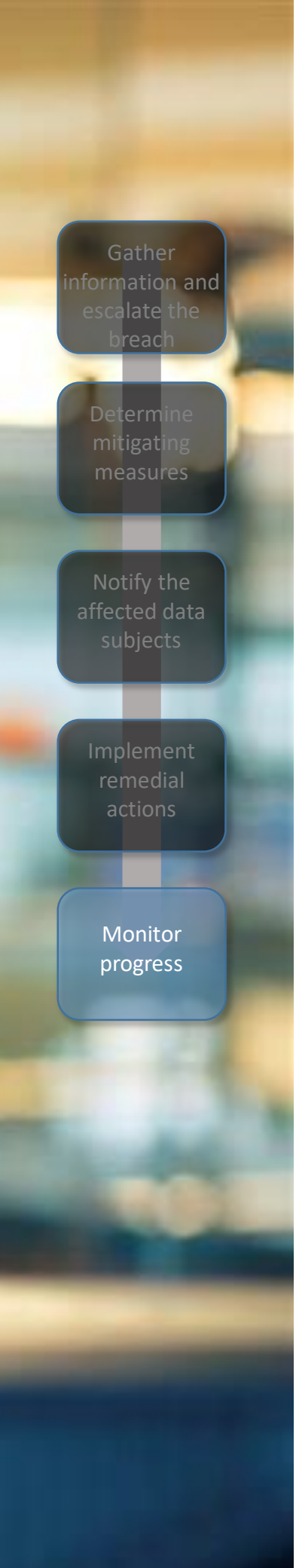
i. Is the data breach an isolated incident, or is it a systematic or persistent problem? For example, did the incident occur even though the relevant employees had followed the routine practices or internal guidelines? If it is a systematic or persistent problem, the responsible department must review the existing guidelines and make any necessary amendments. It may also be necessary to fix the existing (or even bring in new) equipment or IT infrastructure to tackle the issue.

ii. Did the incident involve a massive loss of customers' personal data, which may attract public attention? If so, those who are responsible for dealing with the incident may need to work with the administrative or corporate communications staff to prepare some standard questions and answers so that employees can respond to affected customers and the media. Examples include what kinds of personal data were lost, the approximate number of customers who were affected, what immediate/interim remedial actions have been taken, and what assistance and recommendations are being offered to the affected customers.

iii. Is the incident related to loss of documents or mobile devices that contained personal data?

- If the document or device had been left unattended outside the office premises and the responsible employee subsequently retrieved the document or device from an external party, you should first check whether the relevant personal data could have been read or copied by others.
- If the document or device had been left unattended outside the office premises for a while and the relevant data could be read or copied by others, you should still consider contacting the affected data subjects to alert them about the incident.

Remember to reach out to other relevant experts, such as IT, legal, HR and PR professionals, to get advice before implementing further remedial actions.



E. Monitor the progress of procedures B, C and D and record all relevant incident details

Those who are responsible (e.g. the data protection coordinator of the relevant department) should record the main information about the data breach in a central file. Here are some examples of relevant information:

- Basic information about the incident (as listed in procedure A).
- The remedial and additional precautionary measures that have been taken.
- Reviews that have been performed since the incident (e.g. on damages to your company and your customers).
- Any changes to the daily workflow or business operations to avoid a similar incident occurring.
- If the incident was the fault of an external data processor or service provider, whether the responsible department has reviewed the procedure and criteria for appointing data processors for similar work in the future, and whether your company will terminate the contract of that data processor.

5

Managing contracts with external data processors

If you have to engage an external service provider (data processor) to handle personal data on behalf of your company, you are recommended to adopt contractual means to prevent the data processor from unauthorised or accidental access to, processing of, erasure of, loss of or use of the relevant personal data. You are also recommended to use contractual means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing.

Here are some examples of data protection requirements to include in the relevant service contracts to regulate data processors:

- The security measures required to be taken by the data processor to protect the relevant personal data and obligating the data processor to comply with the data protection principles in the Ordinance.
- Timely return, destruction or deletion of the personal data when it is no longer required for the purpose for which it is entrusted by your company to the data processor.
- Data processor must not use the relevant personal data for any purposes other than the purposes as stipulated on the relevant service contract (including disclosure of the relevant personal data to third party without the consent given by your company);.
- Data processor must not subcontract the service that it has been engaged to provide unless it has obtained prior consent from your company.
- Immediate reporting of any security breaches/data leak incidents to your company, and to take appropriate remedial action.
- Data processor must have its personal data protection policies and procedures in place, and provide relevant training to its staff.
- Data processor to indemnity/compensate your company for violating any data protection obligations.

Appendix 1

The six data protection principles under the Ordinance

The six data protection principles (DPPs) are listed in Schedule 1 of the Ordinance. In summary:

DPP 1 – purpose and manner of collection of personal data

Personal data must be collected for a lawful purpose. The purpose of collection must be directly related to a function or activity of the data user. The data collected should be adequate but not excessive in relation to that purpose.

When personal data is collected from an individual person (the data subject) for a particular purpose(s), that person must be provided with information which includes:

- the purpose(s) for which the data is to be used;
- the classes of persons to whom the data may be transferred;
- whether it is obligatory or voluntary for the data subject to supply the data;
- the consequences arising if the data subject fails to supply the data; and
- data subject's rights to request access to and correction of his own data.

Data users may provide a personal information collection statement ("PICS") which contains the above information to the relevant data subjects.

DPP 2 – accuracy and duration of retention of personal data

Data users have to take practicable steps to ensure that the data held is accurate and up-to-date. They should not keep the data for any longer than is necessary to fulfil the purpose for which the data was collected.

If a data user engages a data processor (e.g. an external service provider) for handling personal data on his behalf, that data user should adopt contractual or other means to ensure that his appointed data processor will not keep the data for longer than is necessary for processing it.

DPP 3 – use of personal data

Personal data must NOT be used for any purpose other than the one mentioned at the time the data was collected (or for a directly related purpose) UNLESS the relevant data subject has given his prescribed consent to the data user. Prescribed consent means express consent given voluntarily by the data subject.

Appendix 1 (Cont'd)

DPP 4 – security of personal data

Data users must take proper security measures to protect the personal data they have collected from unauthorised or accidental access, processing, erasure or use by other people. If a data user engages a data processor (e.g. an external service provider) to handle personal data on his behalf, that data user should adopt contractual or other means to ensure that his appointed data processor will also comply with the data security requirements.

DPP 5 – information to be generally available

Data users must be transparent in their policies and practices about how they handle personal data. They may formulate and publish a privacy policy statement that contains information such as the types of personal data collected, the purposes of collection, accuracy, the retention period, the security measures taken and the channels through which data subjects can submit their data access and data correction requests.

DPP 6 – access to personal data

A data subject has the right to ask a data user whether or not that data user holds any of his personal data and to request a copy of such personal data. If the data subject found that the data contained therein is inaccurate, he can further request the data user to correct the data record.

The data user must comply with the access and correction requests within a statutory period of 40 days. If the data user rejects the relevant request, he must also provide a reply stating the reasons of refusal within 40 days.

Violation of a DPP

If a data user violated a DPP, the PCPD may issue an enforcement notice which compels that data user to take relevant remedial actions. Failing to comply with an enforcement notice issued by PCPD is an offence.

Data access and correction requests are also regulated under Sections 17A– 25 of the Ordinance. Non-compliance with a data access/correction request may also incur criminal liability.

For more information about these offences, see Appendix 2.

Appendix 2

Some major offences relating to breaches of the Ordinance

Failing to comply with an enforcement notice

Failing to comply with an enforcement notice issued by PCPD is an offence which may result in a maximum fine of $50,000 and imprisonment for 2 years, with a daily penalty of $1,000 if the offence continues after the conviction. Subsequent convictions can result in a maximum fine of $100,000 and imprisonment for 2 years, with a daily penalty of $2,000 if the offence continues after the conviction (see section 50A of the Ordinance).

Failing to respond to data access and correction requests

Failing to respond to a data access or correction request within the 40-day statutory period may result in a maximum fine of $10,000 (see section 64A of the Ordinance).

Using personal data for direct marketing

The maximum penalties for violating the notification, consent and opt-out requirements are a fine of $500,000 and imprisonment for 3 years (see sections 35C, 35E, 35F and 35G of the Ordinance).

Disclosing personal data which is obtained without consent from the data user

A person commits an offence under section 64 of the Ordinance if:

i. he discloses any personal data of a data subject which is obtained from a data user without that data user's consent with the intention to: obtain gain (whether for his own or another person's benefit) or to cause loss to the relevant data subject (note); or

ii. he discloses, irrespective of his intent, any personal data of a data subject which is obtained from a data user without that data user's consent, and such disclosure causes psychological harm to the data subject.

(Note: Not only monetary "gain" or "loss" but also covers gain or loss in other property/asset.)

An example for (a) is that an employee steals customers' personal data from his employer and sells those data to another person for a reward. An example for (b) is that an employee steals personal data of his colleague from his company's database and then openly publishes the data for retaliation. The maximum penalties for this offence are a fine of $1,000,000 and imprisonment for 5 years.

Appendix 3

Introduction to the European Union's General Data Protection Regulation

The General Data Protection Regulation (GDPR) (effective from May 2018) has extra-territorial application, which means that your company may be regulated by the GDPR under certain pre-conditions even if your company is NOT established in an EU member state.

Article 3(2) of the GDPR stipulates:

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

In other words, a company which is not established in EU may still be regulated by the GDPR if (i) it collects personal data of an individual who situates in a EU member state; AND (ii) it offers products or services targeting on the EU market OR it monitors the behavior of persons which takes place in a EU member state.

Some major requirements imposed by the GDPR

The following list aims to draw your attention to some of the main requirements for companies that are regulated by the GDPR. It is not a full list. For more details, please seek legal advice.

- Accountability: Data users are required to implement technical and organizational measures to ensure compliance. (e.g. devise appropriate data protection policies, conduct data protection impact assessment for high risk projects)

- Data breach notification: If a data breach incident occurred, the data user has to notify the relevant data protection authority not later than 72 hours after having become aware of it (unless an exemption provision applies). And for high risk incidents, the data user is also required to notify the affected data subjects.

Appendix 3 (Cont'd)

Some major requirements imposed by the GDPR (Cont'd)

- Sensitive personal data: Categories of such data under the GDPR include - ethnic origin, political opinions, religious beliefs, trade union membership, biometric data and health data, etc. Processing sensitive personal data is allowed only under specific circumstances (e.g. when the data subject has given explicit consent for your company to process their data for specified purposes, when processing is necessary for the purposes of employment and social security, or when processing is necessary for reasons of public interest in the area of public health).

- Prior consent: Data users need to seek prior consent from data subjects when collecting their personal data unless the data will be used for certain prescribed purposes (e.g. processing of data is necessary for compliance with a legal obligation or for the performance of a contract).

- Right to be forgotten: The data subjects have the right to obtain from the data users the erasure of their personal data under certain conditions (e.g. the personal data are no longer necessary in relation to the purposes for which they were collected or the personal data have been unlawfully processed by the data users).

- Penalties: the relevant data protection authorities can impose administrative fines on data users of up to €20 million or 4% of annual worldwide turnover, whichever is higher.

HOW BDO CAN HELP: DATA PRIVACY SERVICES

Managed services

- Individual rights administration
- Privacy by design operations
- Maturity assessments
- Privacy watch
- External DPO or internal DPO support

Assessment

- Data privacy readiness assessment
- Data privacy audit / due diligence
- Annual privacy health check
- Data mapping / data flow diagramming
- Data protection assurance / certification

Implementation and remediation

- Data privacy strategy and implementation
- Privacy project management
- Privacy notices, policies and procedures development
- Technical controls implementation
- Third-party processor remediation
- Data minimisation, retention, erasure and classification policies, and process development

Technology support

- Design and review of planned and existing architecture. 'Data privacy by design'
- Data privacy impact assessments & implementation of technical measures
- Data subject rights management
- Data privacy management tools: tool / software selection plan, design & implementation of tools
- Data masking & data encryption tool
- Security assessments: vulnerability scanning, penetration testing, ethical hacking & social engineering

Other support

- Advice on data subject requests and data breaches
- Advice on contractual arrangements with third parties
- International data transfers policies and registers development

BDO CONTACT

If you have any questions, comments or suggestions, please contact us. To learn more about BDO Risk Advisory Services, please visit

www.bdo.com.hk/en-gb/services/advisory/risk-advisory

RICKY CHENG
Director and Head of Risk Advisory
rickycheng@bdo.com.hk

PETER PANG
Director
peterpang@bdo.com.hk

www.bdo.com.hk

BDO Limited 香港立信德豪 BDO Limited 香港立信德豪