Guidance Note on

Data Security Measures for Information and Communications Technology

PCPD
HK

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Table of Contents

1 Introduction

The increased digitisation of data and interconnection of information and communications technology ("ICT"), together with the increasing value of data, have exacerbated personal data security risks. This is evidenced by the upward trend in the number of data security incidents reported both in Hong Kong and other jurisdictions. Personal data privacy and data security are closely connected – personal data privacy will be jeopardised if data security fails and personal data falls into the wrong hands. The impact of a data security incident – both in terms of reputational damage and financial cost – could be devastating to a data user of any size, from small and medium-sized enterprises ("SMEs") to multinational companies.

Furthermore, a robust data security system is an essential element of good data governance, which is increasingly considered an integral part of an organisation's overall corporate social responsibility. It is in this light that the Office of the Privacy Commissioner for Personal Data ("PCPD") has always stressed the importance of accountability in the Privacy Management Programme advocated by the PCPD, the key components of which incorporate organisational and management commitment, data security, and the handling of data breaches.[1]

This Guidance Note aims at providing data users with recommended data security measures for the ICT industry to facilitate their compliance with the relevant requirements under the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("PDPO"). It also provides data users with pointers towards good practices in strengthening their data security systems.

[1] For further information on PCPD's Privacy Management Programme, please see PCPD 's dedicated website at https://www.pcpd.org.hk/pmp/guide.html.

The PCPD is mindful that the steps required of a data user to protect personal data may vary from case to case, and therefore does not seek to provide a "one-size-fits-all" approach for data users in managing data security. Data users should consult their own data security experts and legal advisers on whether the relevant requirements under the PDPO are met.

The data security measures mentioned in this Guidance Note are for general reference only. The PCPD makes no explicit or implied warranties that the adoption of all or part of the measures will offer adequate security to personal data, or will adequately meet the requirements under the PDPO.

2 Requirements under the PDPO

2.1 Requirements on Data Security

Security

Data Protection Principle ("DPP") 4(1) of Schedule 1 to the PDPO requires a data user to take "*all practicable steps*" to ensure that any personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to:

(i) the kind of data and the harm that could result if any of those things should occur;

(ii) the physical location where the data is stored;

(iii) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(iv) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(v) any measures taken for ensuring the secure transmission of the data.

"*Practicable*" is defined to mean "*reasonably practicable*"[2]. It is incumbent upon a data user to show that, in the event of data breaches, all reasonably practicable steps have already been taken to safeguard the security of personal data. What "*reasonably practicable*" steps are will hinge on the facts of each case.

[2] Section 2(1) of the PDPO.

In assessing whether "*all practicable steps*" have been taken by a data user to safeguard the security of personal data in its possession or control, the PCPD will adopt a totality approach, taking into account the following factors (which are non-exhaustive and the weight of each factor varies between cases):

(i) volume, kind and sensitivity of the personal data involved, and the harm that could result in the event of a data security incident[3];

(ii) physical location where the data is stored[4];

(iii) nature and complexity of the ICT used[5];

(iv) whether security measures are sufficiently robust in relation to the resourcefulness of the data user concerned[6];

(v) familiarity of the data security issues in question among the ICT community and the relevant industry, and the availability of solutions[7]; and

(vi) state of development of ICT and data security[8].

For PCPD's recommended data security measures for ICT, please refer to Part 3 of this Guidance Note.

[3] DPP 4(1)(a) of Schedule 1 to the PDPO is relevant, which requires an organisation to take into account the kind of data and the harm that could result if a data security incident occurs. The harm that may result from a data security incident depends heavily on the volume and sensitivity of the personal data involved. The steps required to be taken must be proportionate to the degree of sensitivity of the data and the harm that may result from accidental or unauthorised access to such data. For example, a leak of a high-volume of sensitive personal data is likely to result in significant harm to the affected individuals. Hence, stronger and more stringent security measures are warranted to prevent the leak.

[4] See DPP 4(1)(b) of Schedule 1 to the PDPO. For example, if the premises in which the personal data is stored are highly accessible, enhanced security measures have to be implemented to restrict access to the data.

[5] As regards the nature of an information and communications system, DPP 4(1)(c), (d) and (e) of Schedule 1 to the PDPO are relevant. As regards the complexity of an information and communications system, a complex system usually warrants stronger security measures than a simple system because the former has greater exposure to vulnerabilities. Whether a system is online or offline is also relevant. An online system tends to be more susceptible to data security incidents and warrants stronger security measures.

[6] For example, the PCPD may accept that the data security measures adopted by a small enterprise are not as sophisticated as a big corporation because it may not be reasonably practicable for the small enterprise to do so. However, this does not mean that a small enterprise will be excused for being lax in data security.

[7] For example, failure to identify and patch a commonly known exploitable vulnerability may well be a breach of the data security obligation under the PDPO.

[8] For example, with the continuous advancement of ICT and evolvement of cyberattacks, an organisation should timely update and upgrade its ICT to ensure their security.

2.2 Other Relevant Requirements under the PDPO

Collection Purpose & Means

While DPP 4 creates an explicit legal requirement on the security of personal data, other provisions of the PDPO also have a bearing on data security. On the cardinal principle of data minimisation, DPP 1(1) provides that only an adequate but not excessive amount of personal data should be collected in relation to the purpose for which data is collected. It can be generally understood that the lesser amount of data is collected or held by a data user in the first place, the lesser exposure to security risk there may be in future.

Accurary & Retention

On data retention, DPP 2(2) requires a data user to take "*all practicable steps*" to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used. Similarly, section 26 of the PDPO requires a data user to take "*all practicable steps*" to erase such personal data when the data is no longer required (subject to prescribed exceptions[9]). Implementing data retention policies to ensure the timely deletion of personal data that is no longer needed can help reduce the risk of data breaches. The less data held by a data user, the less exposure to attack and vulnerability.

DPP 2(3) and DPP 4(2) require data users to adopt contractual or other means to ensure that any data processor engaged by them also complies with similar requirements in respect of data security and data retention. For recommended contractual obligations to be imposed on data processors and recommendations on "*other means*" of compliance, data users may refer to the Information Leaflet "Outsourcing the Processing of Personal Data to Data Processors"[10] published by the PCPD.

The security of personal data is important throughout the data cycle. The above is not an exhaustive list of compliance requirements on data security under the PDPO.

[9] The exceptions under section 26 of the PDPO are where:
(a) any such erasure is prohibited under any law; or
(b) it is in the public interest (including historical interest) for the data not to be erased.

[10] Available at https://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf.

3 Recommended Data Security Measures for ICT

Recommended Data Security Measures for ICT in 7 Areas

1. Data Governance and Organisational Measures
2. Risk Assessments
3. Technical and Operational Security Measures
4. Data Processor Management
5. Remedial Actions in the event of Data Security Incidents
6. Monitoring, Evaluation and Improvement
7. Other Considerations

3.1 Data Governance and Organisational Measures

Policy and Procedures

A data user should establish clear internal policy and procedures on data governance and data security, covering the following areas:

(i) respective roles and responsibilities of staff in maintaining the information and communications systems and safeguarding data security;

(ii) data security risk assessments;

(iii) accessing data in and exporting data from the information and communications systems;

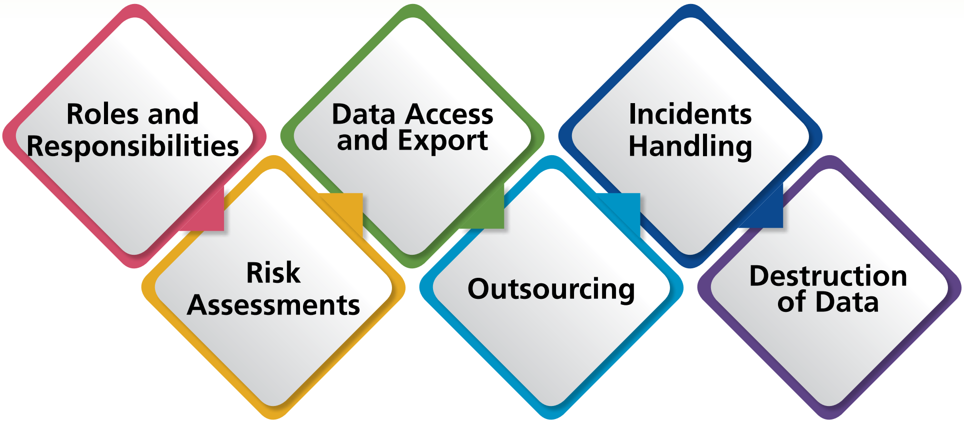
(iv) outsourcing of data processing and data security work;

(v) handling data security incidents, including an incident response plan[11] and reporting mechanism; and

(vi) destruction of data that is no longer necessary for the original purposes of collection or related purposes.

[11] A data security incident response plan is a plan comprising procedures, protocols and guidelines to enable an organisation to respond to, and recover from, data security incidents in a way to minimise damage.

Diagram 1 Internal Policy and Procedures on Data Governance and Data Security



A data user may make reference to the standards and best practices set by reputable organisations (such as ISO/IEC 27000 family of Information Security Management Systems standards), as well as the guidance or recommended practices issued by relevant authorities both locally and in other jurisdictions[12], in assessing and establishing data governance and data security policies. In particular, ISO/IEC 27701:2019 provides detailed guidance for establishing, implementing, maintaining and continually improving a privacy information management system in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002. However, it should be emphasised that the adequacy of security measures will depend on the circumstances of each case.

A data user should review and revise its policies and procedures on data governance and data security periodically and in a timely manner based on prevailing circumstances, such as new industry standards and new threats to data security.

[12] For example, the Personal Information Security Specification (GB/T 35273-2020) of the Mainland, which took effect from October 2020, sets out the technical standards on data security measures at various stages of the data life cycle.

Manpower

A data user should appoint suitable personnel in a leadership role to bear specific responsibility for personal data security (such as a Chief Information Officer, a Chief Privacy Officer or an equivalent person), and should provide appropriate staffing levels for ICT, including ICT security. A data user should have guidelines setting out:

(i) the life cycle of the personal data handled by the data user, from its collection to its destruction;

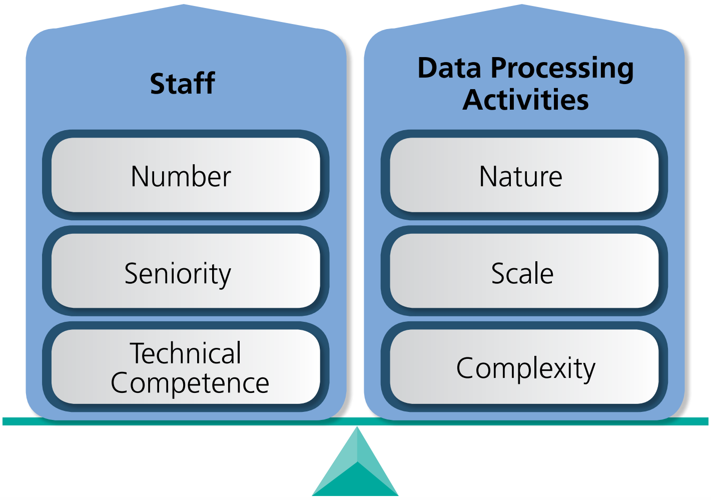
(ii) roles and responsibilities of relevant staff;

(iii) lines of authority for decision-making; and

(iv) accountability and power of oversight concerning access and transfer of personal data.

The number, seniority and technical competence of the staff members allocated for data security should be proportional to the nature, scale and complexity of the ICT and the data processing activities, as well as the data security risks.

Diagram 2 **Proportionate Staff Allocation**



A data user should also be mindful of the prudence and integrity of staff members in order to prevent data breaches caused by human errors or insider attacks. A data user may include confidentiality obligation in employment contracts where appropriate.

Case 1

In a compliance check case[13] published by the PCPD, a toy maker, after a cyberattack, formed a Data Security Governance Board chaired by the Group Chairman to decide on matters concerning data security policy, oversee the policy's implementation, and review the policy periodically.

Training

Sufficient training should be provided for staff members at induction and regularly thereafter to ensure their familiarity with the requirements under the PDPO and the data user's data security policies and procedures. The types of training may include:

(i) effective password management;

(ii) principles and proper use of encryption software;

(iii) principles and proper use of portable storage devices and remote access tools;

(iv) principles of data sanitisation and the proper use of data sanitisation tools;

(v) detecting and being cautious of suspicious hyperlinks, QR codes, and attachments which may direct the user to harmful contents;

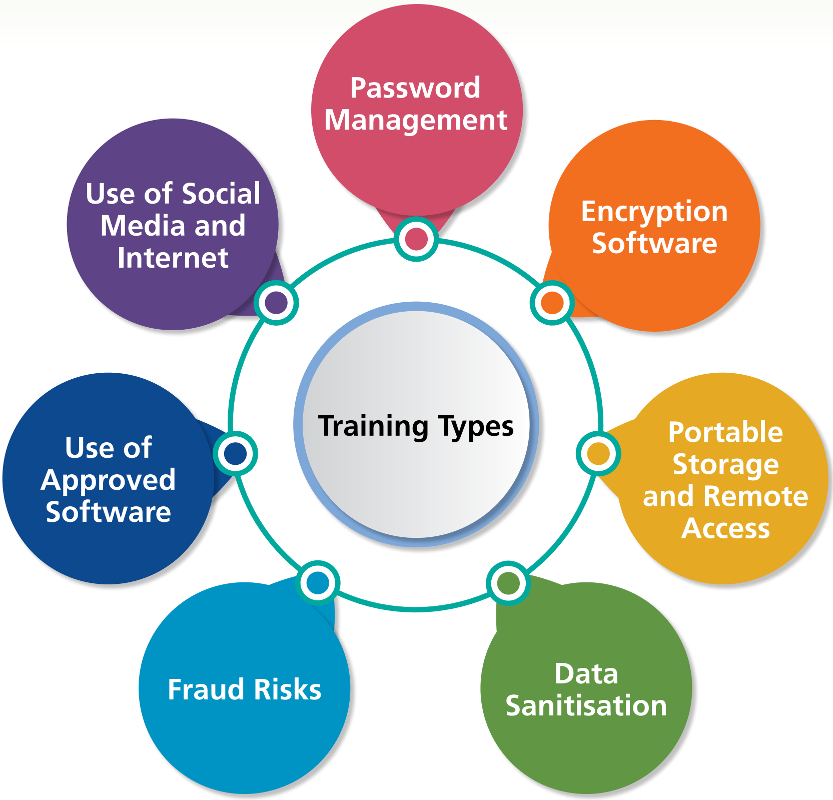
(vi) risks presented by social engineering, phishing emails, ransomware or fake websites;

(vii) use of software that has been approved internally by the data user, but not otherwise; and

(viii) appropriate use of social media and the internet in general.

[13] Details of the case can be found in the PCPD's Annual Report 2016-17, pages 38-39: https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport17_full.pdf.

Diagram 3 Types of Training to be Provided to Staff Members



Another measure that could be incorporated as part of data security training is to conduct fire-drills to reinforce a sense of vigilance amongst employees. For example, after providing training on phishing scams, organisations could conduct a "phishing attack campaign" with mock phishing-scam intrusions at the workplace, in order to raise the alert levels amongst employees against scams. This will help to erect a "human firewall" against the latest social-engineering ploys of cybercriminals.

3.2 Risk Assessments

A data user should conduct risk assessments on data security for new systems and applications before launch, as well as periodically thereafter pursuant to established policy and procedures.

SMEs which may not have the relevant expertise should consider engaging third party specialists to conduct security risk assessments.

Results of risk assessments should be regularly reported to senior management.

A data user should keep inventory of the personal data under its control, and assess the nature of such data and the potential harm arising from leakage of such data. In particular, the collection of sensitive data[14] should be conservatively considered and minimised, and subject to more robust protection (such as storing in a separate data enclave in encrypted form).

Security risks identified in risk assessments should be addressed promptly.

3.3 Technical and Operational Security Measures

Based on the nature, scale and complexity of the ICT and data processing activities, as well as the results of risk assessments, a data user should put in place adequate and effective security measures to safeguard the information and communications systems and personal data in its control or possession.

A non-exhaustive list of technical and operational measures that a data user may consider putting in place to ensure data security is outlined below for reference purposes. It may not be necessary to take all these security measures in order to meet the threshold of "*all practicable steps*" as required under DPP 4(1), nor does the adoption of all the measures mean "*all practicable steps*" have been taken. The adequacy of security measures will depend on the circumstances of each case.

Securing Computer Networks

- Adopting physical access controls to limit access to premises, rooms and physical ICT assets such as server rooms and system devices.

- Using security devices or software such as firewalls and/or anti-malware applications to protect computer networks. Software (including mobile apps and anti-malware applications) should be regularly updated to detect new viruses and emerging threats.

[14] In general, sensitive data refers to genetic data, biometric data, or data revealing racial or ethnic origin, political leanings, health status, sex life or sexual orientation. It also includes data which, if not handled properly, may put an individual at significant risks of discrimination or serious harm (such as credit reference data). The PDPO does not distinguish between sensitive and non-sensitive personal data. However, DPP 4(1)(a) requires an organisation to take into account "*the kind of data and the harm that could result*" in the event of a data security incident when formulating its data security measures. Therefore, in practice, DPP 4(1)(a) encompasses the concept of sensitive data.

- Deploying endpoint security software to prevent users from executing unauthorised applications/actions that could create vulnerabilities in the networks.
- Conducting vulnerability scan at the networks, servers and application levels to identify vulnerabilities (and take appropriate follow up actions) at regular intervals.
- Implementing patch management to fix security vulnerabilities in a timely manner.
- Conducting regular checks/reviews to ensure system settings are updated and appropriate for current requirements.
- Logging system activities for detecting and investigating data security incidents.

Case 2

In a compliance check case[15] published by the PCPD, the credit card systems of a hotel group were attacked by a zero-day malware. As a result, the names and credit card numbers of its customers were suspected to have been leaked. Forensic investigations revealed that a hacker utilised a system account with administrative privileges and planted the malware in the systems worldwide in order to gain access to the credit card data.

Subsequent to the incident, the hotel group took various steps to enhance its network security, which included preventing unauthorised code and/or software from being executed on its networks, conducting periodic audits of administrators and remote access accounts, and increasing restrictions on outbound internet connections to protect against malicious traffic.

[15] Details of the case can be found in the PCPD's Annual Report 2015-16, pages 38-39: https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport16_02.pdf.

Database Management

- Separating database servers from web servers by firewalls to protect the internal servers in case the web servers are compromised.
- Keeping and regularly updating personal data inventory to enable informed decisions on the implementation of data security measures.
- Dataset partitioning – breaking a dataset into smaller sub-sets by segmenting out selected attributes, such as sensitive attributes (thus, the segmented data will not be compromised even if the larger database has been compromised).
- Digital watermarking of data file – adding watermark information such as a cryptographic signature which identifies the originator of a dataset and proves the authenticity of the file. This enables investigators to trace the origin of a dataset in the event of a data breach.
- Prohibition against the use of real data for testing.

Access Control

- Adopting the "least privilege" principle to grant as few access rights as possible to complete a task and assign users to appropriate roles (i.e. role-based access control, including restriction of the volume of data to be accessed and the duration of access).
- Adopting effective logical access controls for the information and communications systems by using passwords, firewalls, etc.
- Implementing password management to manage user passwords. This includes enforcing password length, complexity and history, and ensuring that users follow best practices for password security.
- Setting an account lockout threshold policy to limit the number of failed log-in to information and communications systems, and lock out the user accounts for a pre-determined period of time when the threshold has been reached.[16]

[16] An account lockout threshold policy setting determines the number of failed sign-in attempts that will cause a user account to be locked. The user would not be able to access a locked account until it has been reset or until the prescribed lockout period expires.

- Adopting multi-factor authentication or other enhanced access control for high-risk activities (e.g. remote access to information and communications systems and access to sensitive databases).
- Regular review of access rights and timely removal of unnecessary user accounts and access rights (e.g. upon departure or redeployment of staff).
- Disconnecting information and communications systems from the internet or intranet if remote access to the systems is no longer necessary.

Firewalls and Anti-malware

- Implementing Domain Name System ("DNS") firewalls to prevent information and communications systems or users of the systems from connecting to malicious websites.
- Conducting vulnerability assessments and penetration tests regularly (with sufficient frequency), in particular for those internet-facing systems.
- Using anti-malware software to provide real-time protection against various kinds of malware and prevent the spread of malware on the systems.

Protecting Online Applications

- Ensuring that no unnecessary personal data is stored online.
- Disconnecting systems containing personal data from the internet when they are obsolete.

Encryption[17]

- Proper encryption of data in transit and storage, and effective management and protection of the encryption keys.
- Encryption of data in mobile devices (e.g. smartphones) and portable storage devices (e.g. USBs and external drives).

[17] For encryption methods, please also refer to the "Data Protection Guideline" issued by the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") in May 2022, available at https://www.hkcert.org/security-guideline/data-protection-guideline.

- Tokenisation – replacing identifiers and attributes with a different value known only to authorised users (this is appropriate for data fields where the actual values need to be used later, e.g. individuals' names).

- Hashing the data – replacing sensitive values with an algorithmically derived value that is intended to be irreversible. This is appropriate for data fields where the actual values are not intended to be recovered, such as passwords. (Hashing is a different process from ordinary encryption as the hashed output cannot be decrypted to the original data.)

Emails and File Transfers

- Using the "bcc" (blind carbon copy) rather than the "cc" function to distribute emails, so that a recipient's information (email address or name) will not be visible to other recipients.

- Prevention of misuse of email – install tools (e.g. data loss prevention tools) to ensure that email senders double-check before sending any email with potentially risky activities (e.g. containing sensitive data), to prevent any accidental disclosure of data through email.

- Filtering spams or emails with malicious attachments or links.

- Use of end-point security software to prevent transfer of data from the data user's computer to unauthorised portable storage devices, or insecure portable storage devices that do not have encryption function.

- Adding digital watermarks (which embed important data into a document to track its owner using details about the user, time/date of access, the machine used to access it, etc.) to documents with sensitive personal data to help prevent data loss, misuse and unauthorised sharing.

Case 3

In a compliance check case[18] published by the PCPD, a staff member of a hotel inadvertently attached a document containing the data of a few hundred customers in an email reminding them to collect the goods they had ordered. The document was neither encrypted nor password protected.

In retrospect, the hotel could have encrypted all customer data files and added passwords, and should not have allowed all staff members to have access right to its customer data.

Backup, Destruction and Anonymisation

- Backing up systems that contain essential data, and ensuring that recovery mechanisms would effectively restore data that has been lost, or rendered inaccessible by malware/ransomware.
- To erase data securely, the "Purge" action detailed in NIST 800-88 R1 (Guidelines for Media Sanitization) can be adopted. It involves physical or logical techniques that render data recovery impossible even by using advanced laboratory techniques.[19]
- Timely destruction or anonymisation of unnecessary or expired personal data.

Anonymisation

Anonymisation refers to the use of a set of techniques to remove the ability to link (with "reasonable" effort) a piece of data with an identified or identifiable natural person. Rendering personal data "reasonably" anonymised is considered a data security measure. To determine whether data is "reasonably" anonymised, a data user should take account of both objective aspects (e.g. time and technical means required to de-anonymise) and contextual elements that may vary case by case (e.g. rarity of a phenomenon, size of population and volume of data). If the so-called "anonymised" data

[18] Details of the case can be found in the PCPD's Annual Report 2013-14, page 43: https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport14_02.pdf.

[19] Please also refer to the "Data Protection Guideline" published by the HKCERT, available at https://www.hkcert.org/security-guideline/data-protection-guideline.

fails to pass the reasonableness test, then it remains as personal data. Evaluating the robustness of anonymisation relies on three criteria: (1) singling-out (whether an individual can be isolated in a larger group based on the data); (2) linkability (whether two records concerning the same individual can be linked together); and (3) inference (whether unknown information about an individual can be deduced with significant probability). Given the complexity of anonymisation processes, transparency regarding the anonymisation methodology is highly encouraged.

Other References

- The "Guide to Data Protection by Design for ICT Systems[20]" jointly developed by the PCPD and the Personal Data Protection Commissioner of Singapore provides suggestions on the data protection measures that should be considered when developing information and communications technology systems.

- Information about technical assistance on data security is available on the following websites maintained by the Office of the Government Chief Information Officer of the Hong Kong Government:

  - ▶ Cyber Security Information Portal[21]; and
  - ▶ InfoSec[22].

- The Top Ten Project of the Open Web Application Security Project ("OWASP"[23]) provides valuable insights into the common application security risks.

- In light of the increasing prevalence of Internet of Thing ("IoT") technology, the Hong Kong Computer Emergency Response Team ("HKCERT") has published the "IoT Security Best Practice Guidelines"[24] to assist developers in adopting appropriate security measures at the early stage of design and development of IoT devices. The Guidelines may also serve as a reference of security specifications in sourcing suitable IoT solutions.

[20] Available at https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf.

[21] Cyber Security Information Portal: https://www.cybersecurity.hk

[22] InfoSec: https://www.infosec.gov.hk/

[23] OWASP Top Ten Project: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[24] Available at https://www.hkcert.org/blog/implementing-iot-security-best-practice

- The HKCERT has also published a "Data Protection Guideline"[25] which provides holistic guidance on data security throughout the data cycle.

3.4 Data Processor Management

Engaging contractors (i.e. data processors) for processing personal data is increasingly common. Examples of data processors include cloud and data analytics service providers. Under section 65(2) of the PDPO, a data user may be liable for the acts of its agents (including data processors)[26]. DPP 4(2) also provides that a data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to its data processors for processing.

A data user may consider taking the following actions (non-exhaustive) before and when engaging a data processor:

(i) implementing policy and procedures to ensure that only competent and reliable data processors will be engaged[27];

(ii) conducting assessment to ensure that only necessary personal data is transferred to the data processor;

(iii) clearly stipulating the security measures required to be taken by the data processor in the data processing contract;

(iv) requiring the data processor to immediately notify all data security incidents; and

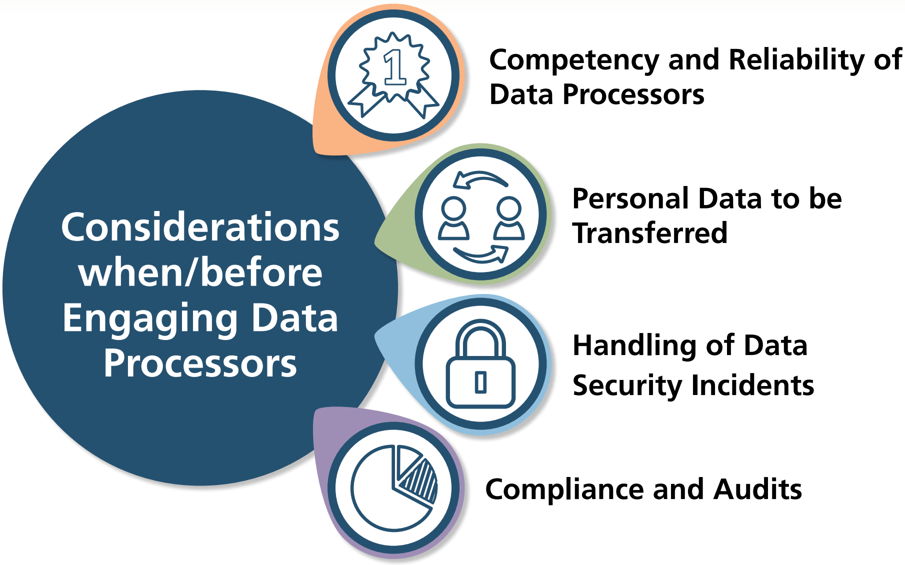
(v) conducting field audits to ensure compliance with the data processing contract by the data processor and impose consequences for breach of contract.

[25] Available at https://www.hkcert.org/security-guideline/data-protection-guideline.

[26] Section 65(2) of the PDPO provides that any act done or practice engaged in by a person as agent (e.g. a data processor) for another person (e.g. a data user) with the authority of that other person (i.e. the data user) shall be treated for the purpose of the PDPO as done or engaged in by that other person as well as by him.

[27] Depending on the circumstances, these possible measures include (1) conducting due diligence before engaging a data processor and (2) checking for reputable and independent certification on the relevant capabilities of a data processor, such as ISO/IEC 27000 family relating to information security management standards.

Diagram 4 Data Processor Management


Considerations when/before Engaging Data Processors
Competency and Reliability of Data Processors
Personal Data to be Transferred
Handling of Data Security Incidents
Compliance and Audits

Case 4

An ex-employee of a bank's contracted call centre in Guangzhou posted personal data of three Hong Kong celebrities to a blog in May 2014.

Subsequent to the incident, the bank prohibited the use of smartphones and cameras in the call centre and required all staff to leave their personal belongings in lockable compartments before entering the call centre. The bank also doubled the patrols in the call centre and required all staff there to complete an e-learning course on data security.

For more details about data processor management, please refer to the information leaflet "Outsourcing the Processing of Personal Data to Data Processors[28]" issued by the PCPD.

[28] Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf.

3.5 Remedial Actions in the Event of Data Security Incidents

DPP 4(1)(a) provides that all practicable steps must be taken to protect the personal data held by a data user, having particular regard to "*the harm that could result*" in the event of a data security incident. Timely and effective remedial actions taken by a data user after the occurrence of a data security incident may reduce the risks of unauthorised or accidental access, processing or use of the personal data affected, thereby reducing the gravity of harm that may be caused to the affected individuals (i.e. data subjects).

Below are some examples of common remedial actions that a data user may take in the event of a data security incident:

(i) where practicable, immediately stopping the affected information and communications systems and disconnecting them from the internet and other systems of the data user;

(ii) immediately changing the passwords or ceasing the access rights of the users suspected to have caused or contributed to the data security incident;

(iii) immediately changing system configurations in order to control access to the affected information and communications systems;

(iv) notifying the affected individuals without undue delay and providing them with suggestions on possible actions for self-protection;

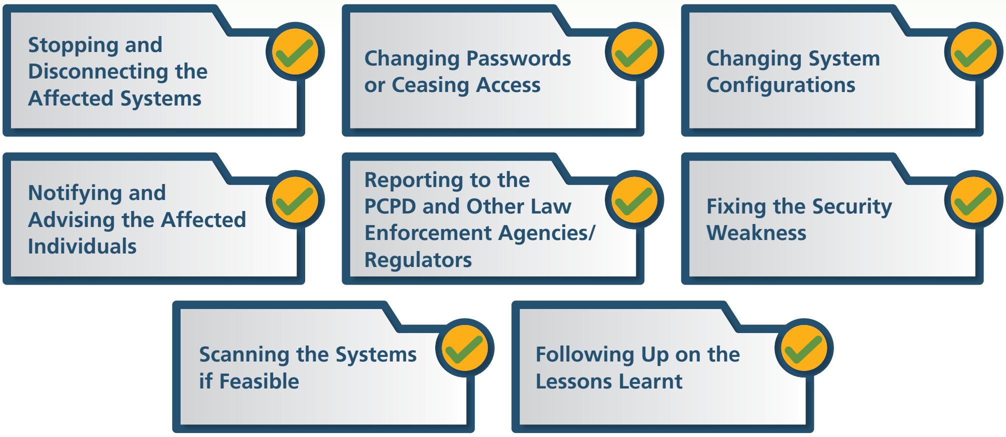
(v) notifying the PCPD and other law enforcement agencies or regulators, where applicable, without undue delay;

(vi) fixing the security weaknesses in a timely manner; and

(vii) where practicable and to the extent that it does not affect future forensics analysis, scanning the information and communications systems for any other unknown security vulnerabilities.

A data user should also take into consideration lessons learnt from a data security incident to review and strengthen its overall data governance and data security measures.

Diagram 5 Common Remedial Actions in the Event of Data Security Incidents



Stopping and Disconnecting the Affected Systems

Changing Passwords or Ceasing Access

Changing System Configurations

Notifying and Advising the Affected Individuals

Reporting to the PCPD and Other Law Enforcement Agencies/ Regulators

Fixing the Security Weakness

Scanning the Systems if Feasible

Following Up on the Lessons Learnt

For detailed guidance concerning handling of data breaches, please refer to the "Guidance on Data Breach Handling and the Giving of Breach Notifications"[29] issued by the PCPD.

3.6 Monitoring, Evaluation and Improvement

A data user may commission an independent task force (e.g. an internal or external audit team) to monitor the compliance with the data security policy and evaluate the effectiveness of the data security measures periodically. Improvement actions should be taken for non-compliant practices and ineffective measures.

3.7 Other Considerations

As we move towards digital workplace, it is increasingly common to work away from the office (for instance, work from home or other remote office practices). Under such circumstances, data may need to be transferred out from a data user's information and communications systems, creating a variety of data security issues.

[29] Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf.

Cloud Services

Computing and data storage services offered by third-party cloud service providers can reduce the cost and increase the flexibility of a data user's information and communications system. Hence the use of cloud services is increasingly common. Cloud service providers are generally data processors, and the security measures under Part 3.4 of this publication shall apply.

Unlike conventional data processors, a cloud service provider may not offer tailor-made services to a data user. Being one of the many customers using standardised cloud services, a data user usually does not have effective control over the operations and security controls of the cloud service provider. Nonetheless, a data user remains primarily responsible for the security of personal data entrusted to a cloud service provider.

To ensure the security of the cloud-based environment and safeguard the security of personal data, a data user should take the following measures when using cloud services:

(i) assessing the capability of cloud service providers, and seeking formal assurance from the providers on the security controls of the cloud-based environment;

(ii) setting up strong access control and authentication procedures for the cloud-based environment, such as strong password policies, multi-factor authentication, proper documentation and regular review of access rights; and

(iii) reviewing the cloud-based security features available and applying the features as appropriate; not merely relying on the default security settings.

Diagram 6 **Considerations when Using Cloud Services**

Security Features Available
Capability of Service Providers
Strong Access Control and Authentication Procedures

Bring Your Own Device ("BYOD")

BYOD refers to an organisational policy that allows employees to use their own devices (e.g. smart phones, notebook computers) to access the data user's systems and process the data held by the data user. In doing so, the data user is effectively transferring data from a secure corporate system to an employee's less secure device, over which the data user has far less effective control. Meanwhile, the data user remains fully responsible for complying with the PDPO in respect of the personal data transferred to its employees' devices.

A data user should therefore establish administrative and technical measures to ensure that such personal data is protected. A data user should also reinforce the effectiveness of these measures through written policies and training. A data user may deploy the following security measures, among others, for implementing a BYOD policy to comply with the data security obligations under the PDPO:

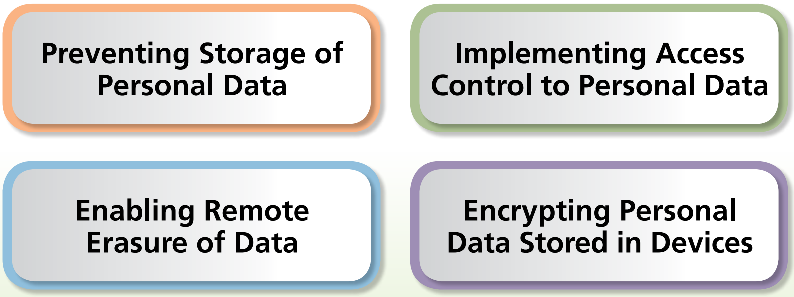
(i) preventing data user-collected personal data from being stored in BYOD equipment, where possible;

(ii) controlling access to personal data stored in BYOD equipment (e.g. requiring separate log-in in addition to the screen locks of employees' smart phones);

(iii) encrypting personal data stored in BYOD equipment by using encryption method that is not built-in for the BYOD equipment; and

(iv) installing appropriate software on BYOD equipment that will allow remote erasure of data stored within the equipment, in case the BYOD equipment is lost or stolen.

Diagram 7 **Possible Security Measures when Implementing BYOD Policy**



Preventing Storage of Personal Data

Implementing Access Control to Personal Data

Enabling Remote Erasure of Data

Encrypting Personal Data Stored in Devices

For more information about BYOD, please refer to the information leaflet "Bring Your Own Device (BYOD)"[30] issued by the PCPD.

Portable Storage Devices ("PSDs")

Commonly used PSDs include portable hard disks, USB flash drives and SD cards. PSDs provide a convenient means to store and transfer data. The use of PSDs enables a large amount of personal data to be quickly and easily copied and transferred outside of a data user's secure corporate system, increasing the risk of data security incidents.

Data users should avoid the use of PSDs to store personal data as far as practicable. If the use of PSDs is necessary, the following security measures, among others, may be implemented to comply with the data security obligations under the PDPO:

(i) establishing a policy to set out (1) the circumstances under which PSDs may be used; (2) the types and amount of personal data that may be transferred to PSDs; (3) the approval process for the use of PSDs; and (4) the encryption requirements for the data transferred to PSDs, etc.;

(ii) use of end-point security software to prevent transfer of data from the data user's information and communications systems to insecure (e.g. without encryption function) or unauthorised PSDs;

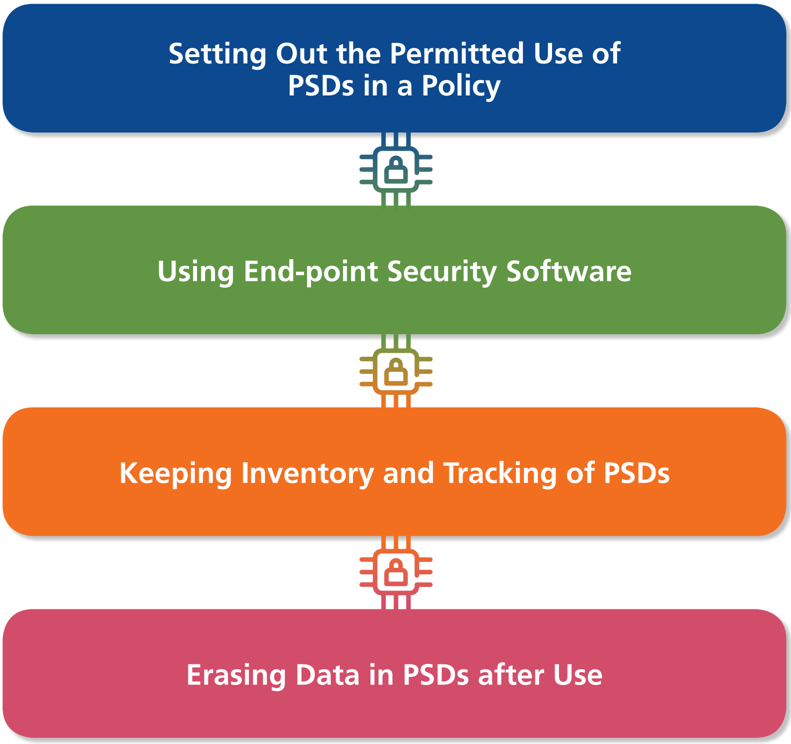
(iii) keeping inventory of PSDs and tracking their uses and whereabouts; and

(iv) erasing data in PSDs securely after each use[31].

[30] Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/BYOD_e.pdf.

[31] Data deleted from PSDs may be easily recovered and become readable again by special software. Proper data sanitisation, by which data is permanently and irreversibly removed from a memory device, is recommended.

Diagram 8 Possible Security Measures for the Use of PSDs



Setting Out the Permitted Use of PSDs in a Policy

Using End-point Security Software

Keeping Inventory and Tracking of PSDs

Erasing Data in PSDs after Use

For detailed guidance concerning the use of PSDs, please refer to the "Guidance on the Use of Portable Storage Devices"[32] issued by the PCPD.

[32] Available at https://www.pcpd.org.hk/english/resources_centre/publications/files/portable_storage_e.pdf.

4 Annex: Recommended Data Security Measures at a Glance

4.1 Data Governance and Organisational Measures

- Establishing Clear Internal Policy and Procedures on Data Governance and Data Security
- Appointing Suitable Personnel in a Leadership Role for Personal Data Security with Appropriate Staffing Levels for ICT Security
- Providing Staff Members with Sufficient Training on PDPO, Data Security Policies and Procedures

4.2 Risk Assessments

- Conducting Risk Assessments on Data Security for New Systems and Applications before and after Launch
- Keeping Inventory of the Personal Data under their Control, and Assessing the Nature and Risk of Such Data

4.3 Technical and Operational Security Measures

- Securing Computer Networks
- Database Management
- Access Control
- Firewalls and Anti-malware
- Protecting Online Applications
- Encryption
- Emails and File Transfers
- Backup, Destruction and Anonymisation

4.4 Data Processor Management

- Competency and Reliability of Data Processors
- Personal Data to be Transferred
- Handling of Data Security Incidents
- Compliance and Audits

4.5 Remedial Actions in the Event of Data Security Incidents

- Stopping and Disconnecting the Affected Systems
- Changing Passwords or Ceasing Access
- Changing System Configurations
- Notifying and Advising the Affected Individuals
- Reporting to the PCPD and other Law Enforcement Agencies/ Regulators
- Fixing the Security Weakness
- Scanning the Systems if Feasible
- Following up on the Lessons Learnt

4.6 Monitoring, Evaluation and Improvement

- Monitoring and Evaluating the Compliance with and the Effectiveness of the Data Security Policy and Measures Periodically
- Taking Improvement Actions

4.7 Other Considerations

Cloud Services

Bring Your Own Device (BYOD)

Portable Storage Devices (PSDs)

PCPD
H K

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

私隱公署網頁
PCPD Website

下載本刊物
Download
this publication

香港灣仔皇后大道東248號大新金融中心13樓1303室
Unit 1303, 13/F., Dah Sing Financial Centre,
248 Queen's Road East, Wanchai, Hong Kong

電話 Tel : 2827 2827
傳真 Fax : 2877 7026
電郵 E-mail : communications@pcpd.org.hk
網站 Website : www.pcpd.org.hk

二零二二年八月初版 First published in August 2022

環保紙印刷 Printed on recycled paper