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

Guidance Note

Guidance on the Use of Portable Storage Devices

Introduction

Portable storage devices ("**PSDs**") such as USB flash memories or drives, notebook computers or backup tapes provide a convenient means to store and transfer personal data. However, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policy and practice.

This Guidance Note seeks to assist organisational data users in addressing the personal data protection aspects of using PSDs.

What are PSDs?

In general, any device that is portable with storage or memory and on which users can store data is a PSD. PSDs are not limited to the obvious USB flash cards. They also include other types of device such as tablets/notebook computers, mobile phones, smartphones, personal digital assistants, portable hard drives, backup tapes and optical discs such as DVDs.

Legal Requirement on Data Security

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

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

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

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

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

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

Data users should, therefore, take steps to manage the security risks associated with the use of PSDs in order to comply with DPP4(1).

DPP4(2) further requires that if a data user engages a data processor[1], whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

[1] A "data processor" is a person who (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes.

Understanding the Risks

The use of PSDs means that large amounts of personal data can be quickly and easily copied to such devices without notice. If such PSDs are lost or stolen, unauthorised or accidental access or use of that personal data may result. In extreme cases, even personal data contained in files already deleted or previously stored on reformatted PSDs can easily be recovered.

A Top-down Approach

A top-down approach of first developing an organisation-wide policy should be adopted to manage the risks associated with the use of PSDs. A risk assessment should be carried out to facilitate the formulation of the policy. The risk assessment should at least look into the following areas:

(a) What types of PSDs are used to store personal data?

(b) What kinds of personal data are stored on PSDs and their sensitivity to the persons involved?

(c) Under what circumstances and how often are PSDs used for the storage of personal data?

(d) What is the likely impact on data subjects if a data breach incident involving PSDs occurs?

(e) Are there any controls, administrative or technical, in place for the use of PSDs?

Results of the risk assessment will help to guide the development of the corresponding data protection policy, practical guidelines and easy-to-follow procedures. The whole system must be reviewed and audited regularly to ensure its effectiveness.

Guidelines, Procedures and Training

Unless the organisational policy bans the use of PSDs outright, practical guidelines for users should be developed to assist them in complying with the high-level policy. If users are required to perform technical operations to comply with the organisational policy, then procedures should be drawn up to ensure those operations are performed correctly. For example, step-by-step procedures should be provided to users who are required to use a particular piece of software to encrypt files to a pre-determined encryption standard before they are allowed to be stored on PSDs. These procedures may vary according to the type of PSDs.

Once the policy, guidelines and procedures are formulated, users must be trained to follow the relevant guidelines and procedures, and made accountable for non-compliance.

Documented Policy

Policy concerning the use of PSDs should include or address the issues quoted below, which are for reference only and are not meant to be exhaustive:

Avoidance of Risk

➤ Risks of data breach can be avoided if personal data is not stored on PSDs. Organisations must therefore first evaluate the benefits and risks, and decide whether the use of PSDs should be allowed at all.

➤ If PSDs have to be used for the storage of personal data, organisations must study the feasibility of using internal identifiers instead of HKID Card Number for purposes other than authentication of the identity of individuals in order to mitigate the adverse consequences of any data breach.

- The decision on the scope and level of detail of the data to be stored should be justified. For example, why is it necessary to store the entire database on the PSD when only part of it is to be used? In other cases, why is it necessary to store all the details of an individual from a database when only some skeletal information of an individual is needed?

- Steps must be taken to minimise the security risks involved. Policy decisions should be made on:

  - whether to restrict the type of PSDs to be used with particular regard to the level of security that can be offered by different PSDs;
  - the use only of official PSDs provided by the organisation themselves (i.e. prohibiting the use of private PSDs which could result in the security standards imposed by the organisation not being met, inability to track where personal data is stored and unauthorised access to the personal data due to the shared use of PSDs for business and private use);
  - the specific circumstances of use;
  - the type and amount of personal data allowed to be stored or processed on PSDs;
  - whether there is a need for an approval process for their use;
  - whether users other than employees, such as contractors, agents or volunteers, are allowed to use PSDs;
  - whether to allow the sharing of the same PSD by different persons and by different processes;
  - whether PSDs may be taken away from the premises of the organisation;
  - the mandatory procedures for erasing the data stored on PSDs after use, etc.

- When disposing of PSDs, organisations must ensure that personal data stored on the PSDs is permanently erased. If PSDs are sent for repair or warranty replacement, organisations must ensure that personal data stored on the broken PSDs cannot be retrieved by others or there are explicit contractual agreements with the service provider on how to handle such personal data.

Prevention of Unauthorised Access

- Personal data stored on PSDs should be encrypted as encryption is the most effective means to prevent the data from being accessed by unauthorised persons, which may happen when the PSDs are lost or stolen.

- When carrying out encryption, two aspects of the encryption process should be carefully considered:

  - **Encryption Algorithm** – It determines how complex or difficult it is to convert information to unintelligible form. A strong algorithm should be chosen for encryption. Users should note that some software may offer, by default, a weak algorithm to maintain compatibility with older versions.
  - **Encryption Mechanism** – The best encryption mechanisms are those that would mandate encryption and cannot be bypassed or disabled by users. If encryption cannot be mandated by technology, adequate policy and procedure should be in place to ensure all information stored on PSDs is strongly encrypted.

➤ Encryption protection can be defeated by weak passwords or poor password controls (for example, by writing down password on paper and tacking it next to the PSD). There should be corporate policy and, better still, technical controls to ensure that passwords used for PSDs are complex enough in terms of length and of alphanumeric combination. Organisations should also develop policies or guidelines on other practical issues such as whether to use different passwords for each piece of PSD and whether passwords are disclosed on a need-to-know basis.

➤ Some PSDs, such as phones and tablet computers, support inactivity passwords which serve as access control as distinct from encryption. They should be enabled to deter any unauthorised access attempts.

➤ The practice of securely erasing data held on PSDs via special programmes after each and every use will ensure that data cannot be recovered by others who subsequently use or have access to the PSDs.

➤ PSDs are often left in public places and lost in transit. Organisations should remind users to closely guard their PSDs and develop ways to assist them. For example, they may supply cable locks with notebook computers. Furthermore, organisations should not label their PSDs with the organisation's identity, which may give an indication of the value of the data stored.

➤ In addition to their primary connectivity, some PSDs have other means of connectivity, such as through Wi-Fi, Bluetooth or mobile network. There should be corporate policy to control or restrict the use of these other means of connectivity as they may expose the data contained on the PSDs to the risks of accidental disclosure or malicious attacks. For example, if smartphones with personal data stored are allowed to run mobile apps, will these mobile apps access the personal data stored on the phone and disclose it without the knowledge of the user?

➤ Given the vulnerability of PSDs, if organisations do not have a policy relating to the encryption and prevention of loss of personal data on PSDs, they will generally not be regarded as having taken all reasonably practicable steps under DPP4(1) to prevent unauthorised or accidental access to personal data held on PSDs.

Detection of Risks

➤ Where PSDs are provided by the organisation, there should be guidelines on when those PSDs should be returned for inventory checks. Spot checks should be conducted to confirm that the users are holding and have not misplaced or lost the PSDs provided.

➤ A formal policy on reporting loss of PSD would allow any potential data breach incident to be managed proactively. A mandatory internal reporting requirement for users handling personal data should be in place and users should be made aware of such requirement.

➤ Users must be required to promptly report any loss of PSDs. Some PSDs support remote erasure through mobile networks but if the loss is not promptly reported, the PSDs' SIM cards may be removed before the organisation has the opportunity to erase the stored data.

Keeping Pace with Technology Change

➤ The policy on PSDs should be specific enough so that users know how it is applied to a specific type of PSD. Given the rapid development of technology, such policy should be updated regularly. If a policy only applies to specific PSDs, organisations should take appropriate steps to avoid risks arising from the use of new types of PSDs that may not have been covered by the policy.

Staff Awareness and the Consequence of Non-compliance

- In order to uphold the policy, there should be effective ways to regularly communicate to users the policy requirements of the organisation and the consequence of non-compliance.

Regular Review and Audit

- To keep pace with technological developments, there should be a formal mechanism to re-assess regularly the risks associated with the use of PSDs and to review the relevance and scope of the established policy on PSDs.

- The implementation and compliance level of PSD policy should be audited regularly to gauge its effectiveness.

Technical Controls

A number of technical controls could be used to assist the implementation of PSD policies. Examples are listed below:

End-point Security – End-point security software (software that controls the security of "end-point" devices such as personal computers, mobile phones) can be installed to all computers and controlled centrally to prevent the use of storage devices such as USB storage or optical drives. The most basic ones prohibit the use of those storage devices altogether. More sophisticated ones allow read/write access to an approved list of devices but turn other devices into read-only devices. The most sophisticated ones mandate encryption before such devices can be used. It has been proved that policy-alone measures are not per se effective in stopping users from using unauthorised PSDs so end-point security software should be seriously considered by organisations.

Data Loss Prevention System – Data loss prevention systems detect and block the saving of sensitive information to external storage devices or even sending through email systems.

Inventory Control – Inventory control and stocktaking are important so that the number, types and whereabouts of all PSDs are known. This helps to reinforce the sense of responsibility of all users of PSDs and would assist incident handling strategy in the case of loss.

Erasure/Disposal/Reallocation – Data stored on PSDs should be securely erased after each and every use. Unless there is a built-in system to securely erase data, organisations should deploy the correct software to perform the erasure. For example, software designed for securely erasing hard drives is not effective for erasing USB flash memories.

Data Breach Handling and Notification

Although it is outside the scope of a PSD policy, given the vulnerability of data stored on PSDs, organisations should have a formal data breach handling and notification policy in place. They may refer to the *Guidance Note on Data Breach Handling and the Giving of Breach Notifications*[2] issued by the Commissioner, which can be downloaded from its website.

Engagement of Service Providers

If organisations engage third-party service providers who would handle PSDs containing personal data, whether as part of the organisations' business operations or to handle the repairing or disposal of PSDs containing personal data, the organisations are accountable as principal for the act done or practice engaged in by the service providers in handling the personal data entrusted to them[3].

[2] Available at http://pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf

[3] See section 65(2) of the Ordinance

Furthermore and in accordance with DPP2(3) and DPP4(2), if service providers are engaged by the organisations to process (including to erase) personal data held on PSDs, the organisations must adopt contractual or other means to ensure that the service providers do not keep the transferred personal data longer than is necessary, and to prevent unauthorised or accidental access, processing, erasure, loss or use of the transferred personal data.

For more information on the engagement of service providers, please refer to *Information Leaflet – Outsourcing the Processing of Personal Data to Data Processors*[4] issued by the Commissioner.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address: 12/F, 248 Queen's Road East, Wanchai,
Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

Copyrights

Disclaimer

The information provided in this guidance note is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of the law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and power conferred to the Commissioner under the Ordinance.

[4] Available at http://www.pcpd.org.hk/english/publications/files/dataprocessorsdataprocessors_e.pdf