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. Privacy could easily be compromised if the use of these devices is not supported by adequate data protection policies and practices.

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 and contains storage or memory into which users can store data is a PSD. PSDs are not limited to the obvious USB flash memories. They also include other device types such as tablet/notebook computers, mobile/smart phones, personal digital assistants, portable hard drives and optical discs such as DVDs.

Legal Requirement on Data Security

Data Protection Principle ("**DPP**") 4 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 are protected against unauthorised or accidental access, processing, erasure or other 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 are stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are 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.

Understanding the Risks

The use of PSDs means that large amount of personal data can be quickly and easily copied to such devices without notice. When the PSDs are lost or stolen, unauthorised or accidental access or use of those personal data may result. In extreme cases, even personal data deleted or previously stored in re-formatted 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 risk 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:

- What types of PSDs are used to store personal data?
- What kinds of personal data are stored in PSDs and their sensitivity to the persons involved?
- Under what circumstances and how often are PSDs used for the storage of personal data?
- What are the likely impacts on data subjects if a data breach incident involving PSDs occurs?
- 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 and 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 guidelines 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 in PSDs. These guidelines 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 Policies

Policies 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 are not stored in PSDs. Organisations must 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 details of the data to be stored should be justified. For example, why is it necessary to store the entire database when only part of it is used? In other cases, why is it necessary to store all the details of an individual from a database when only some skeleton information of an individual is needed?
- Steps must be taken to minimise the 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;
  - ✧ whether organisations should only allow the use of PSDs provided by themselves (i.e. prohibiting the use of private PSDs which could result in not meeting the security standards imposed by the organisation, inability to track where personal data are stored and unauthorised access to the personal data due to the sharing of PSDs for private use.);
  - ✧ the specific circumstances of use;
  - ✧ the type and amount of personal data allowed to be stored;
  - ✧ 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 people and by different processes;
  - ✧ whether PSDs may be taken away from the premises of the organisation;
  - ✧ the mandatory procedures for erasing the data in PSDs after use, etc.
- When PSDs are being disposed of, organisations must ensure that personal data stored in the PSDs are permanently erased. If PSDs are sent for repair or warranty replacement, organisations must ensure that personal data stored in 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 in PSDs should be encrypted as encryption remains the most effective means to prevent data from being accessed by unauthorised persons in the event of loss, deliberate attempt to access information or access by accident.
- 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 policies and procedures should be in place to ensure all information stored in PSDs is strongly encrypted.

- Encryption protection can be defeated by weak passwords or poor password controls. There should be policies and, better still, technical controls to ensure that passwords used for PSDs are complex enough in terms of length and of alphanumeric combination. The ways in which these passwords can be remembered, stored and transmitted need careful management too.
- 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 in 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 left in public places and lost in transit very often. 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 seriously consider whether to 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 Wi-Fi, Bluetooth or mobile network, available to them. There should be a policy to deal with the issues associated with such connectivity to avoid accidental disclosure to or malicious attacks from these connectivity. For example, if smart phones stored with personal data are allowed to run mobile apps, will these mobile apps access personal data stored in the phone and disclose them without the knowledge of the user?
- If organisations do not have a policy related to the encryption and prevention of loss of personal data in PSDs, given the vulnerability of PSDs, they will generally not be regarded as having taken all reasonably practicable steps under DPP4 to prevent unauthorised or accidental access of personal data held in 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 the PSDs provided.
- A formal policy on reporting loss of PSD would enable 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 as some PSDs support remote erasure through mobile networks but the SIM cards are often removed long before the organisation is notified of the loss.

Keeping Pace with Technology Change

- The policies on PSDs should be specific enough to enable their users to 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 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 communicate to

users regularly 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 risk associated with the use of PSDs and to review the relevance and scope of the established policies on PSDs.
- The implementation and compliance level of PSD policies 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, optical drives or floppy drives. The most basic ones stop those storage devices from being used altogether. More sophisticated ones allow read/write access to an approved list of devices while turning other devices into read-only devices. The most sophisticated ones mandate encryption before such devices can be used. It has been proved in the past that policy-alone measures are not 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 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 increase the sense of responsibility of using PSDs by all users and would assist the incident handling strategy in the case of loss.

Erasure/Disposal/Reallocation – Data stored in 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 handle the erasure. For example, software designed for securely erasing hard drives are 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 in 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 issued by the Office of the Privacy Commissioner for Personal Data, which can be downloaded from its website.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Enquiry 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