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 Personal Data Erasure and Anonymisation

Introduction

Data users engaged in the collection, holding, processing or use of personal data must carefully consider how to erase such personal data when it is no longer required for the purpose for which it was used.

Furthermore, when disposing storage holding personal, data users must take practicable steps to ensure that the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note also introduces the alternative of anonymisation, which de-identifies personal data to the extent that it is no longer practicable to identify an individual directly or indirectly, in which case the data would not be considered as personal data under the **Personal Data (Privacy) Ordinance** ("**the Ordinance**").

Legal Requirements related to Personal Data Erasure

Section 26 of the Ordinance provides that a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased.

Data Protection Principle ("**DPP**") **2(2)** in Schedule 1 to the Ordinance requires data users 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.

DPP2(3) provides that if a data user engages a data processor, 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 any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

DPP4(1) requires a data user to take all practicable steps to ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use, including the consideration of:

(a) the kind of data and the harm that could result if any of those incidents 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.

DPP4(2) provides that if a data user engages a data processor, 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.

It is clear from **section 26**, **DPP2(2)** and **DPP2(3)** that when personal data is no longer required for the purpose for which it is or is to be used by the data user, it is the responsibility of the data user to erase the data or to prevent it from being kept longer than is necessary.

Although **DPP4** concerns primarily the security of personal data, it also applies to the secure destruction of personal data (or its copy) held in paper forms or in storage devices. For examples, the destruction of paper records or photocopies which contain personal data, or the handling of obsolete information technology storage equipment for disposal or recycling.

Data users should note that contravention of **section 26** of the Ordinance is an offence and offenders are liable to a fine.

The Importance of a Top-Down Approach

An organisation may want to erase data, or to discard the physical records or storage devices with personal data on them for various reasons. A top-down approach is required for the management of data destruction. This necessitates the development of organisation-wide policies, guidelines and/or procedures. Without a top-down approach, records or devices holding personal data may be kept longer than necessary or discarded unnoticed.

Retention and Erasure Policies

In order to comply with **section 26** and **DPP2(2)**, data users should have a personal data retention policy that specifies in detail the retention period of personal data they hold. At the same time, data users should have a personal data erasure policy that sets out specific management practices on how each type of records, digital or physical, is to be identified for erasure.

The erasure policy should also address the requirements listed under **DPP4(1)** that copies of personal data no longer needed (e.g. photocopies of job-application forms after they are used by members of an interview panel) are disposed of properly and securely. It should also address how to safely and securely delete digital or destroy paper records that are no longer required, as well as how to handle obsolete or damaged storage devices.

An erasure record should be maintained as evidence that the erasure policy has been complied with. Such record should document which set of personal data has been deleted or destroyed, when, by whom, and by what method. Care should be taken to ensure that the erasure record itself does not contain personal identifiers (e.g. the destruction record of job-application forms may contain, among other house-keeping information, the number of forms received for a particular post within a particular period but should not contain identifiers such as the names of applicants on the forms).

Safe and Secure Erasure

Guidelines, and in some cases, procedures, should be established on the erasure method to be used for each type of records. The purpose of the erasure is to irreversibly delete or destroy the personal data so that it cannot be recovered. The method used must, therefore, match with the type of storage technology.

For example, in the case of paper records, cross-cut shredding should be used instead of strip shredding so that individual sheets cannot be easily reconstructed.

A decision must be made as to whether the shredded wastes should be specially handled or can be thrown away with normal office waste. Another issue which needs to be considered carefully is whether paper record destruction should be carried out on the organisation's premises or off-site, which would involve transporting personal data outside the data user's premises.

Similarly, in the case of digital records, an appropriate method must be deployed to permanently delete data from each specific type of electronic storage device. Simple file deletion or reformatting of hard drives and USB memory devices are not reliable methods of deletion, as data can be fully recoverable by commonly available third-party software. Instead, it is recommended that dedicated software, such as those conforming to industry standard (e.g. US Department of Defence deletion standards, the DoD 5220.22-M standard), be used to permanently delete data on various types of storage devices, such as hard drives or USB memory devices. Such software may take a long time (in terms of hours) to delete the data stored on a device, but the result is considered safe and secure. For records residing in servers, an appropriate method should be chosen to delete the data, bearing in mind any facilities within the server that can be used to recover removed records or files (such as an "undelete" command that can be used to recover previously erased files in a server).

Physical destruction remains an effective means of deleting electronic records (typically drilling holes through the entire media or putting magnetic media through a degausser to completely randomise its magnetic properties). This is particularly appropriate in cases where the records can no longer be accessed electronically by the data users. Examples in this category include old backup tapes which the data user has no suitable device to read or delete, and hard drives and USB memory devices that appear to be broken. As physical destruction methods will often render the media unusable, they may be considered as the last resort by data users.

Whole-Record Erasure

When personal data is required to be erased in order to comply with **section 26** and **DPP2(2)**, all copies of the personal data must be accounted for in the erasure exercise. This includes all photocopies, backup copies or digital copies of the personal data. The retention policy or erasure policy should specify the means to identify, gather and record all such copies for erasure. In some cases it may not be reasonably practicable to erase individual records contained in backup media when information stored in it has different retention periods (e.g. various records stored in a single backup tape or microfilm roll). In such cases, in keeping with the relevant retention principle, data users should develop management policies or practices to ensure that such information would not be accessed and/or used.

A Holistic Approach

Expiry of retention period and disposal of surplus records/ storage devices are not necessarily the only situations in which data erasure is concerned about. Other less obvious situations may include shipping apparently broken hard drives to a maintenance contractor who offers a new-for-old replacement service. Although such drives may no longer be accessible in the computers or server on the premises of the data user, they could be reinstated, refurbished or resold by the contractor, possibly with data still left in the drive. Steps must be taken to address such risk.

Furthermore, storage devices are being incorporated in all kinds of equipment and come in all shapes and sizes. These include printers and photocopiers with built-in storage capability, and portable storage devices such as smartphones (including their memory cards), USB drives, memory cards for cameras, tablet computers and music players. Organisation should have a formal portable and/or mobile device policy governing, among other things, the use, protection and data erasure of these office properties.

If an organisation allows the use of personal devices (computers, tablets, phones etc.) for work, it must develop

a formal "bring your own device" (BYOD) policy and include in it, among other rules on use and protection, how the data stored in these devices be erased in the event of disposal, loss and/when the owner leaving his/her position.

Retention and erasure polices must also be regularly reviewed to keep pace with work practices and technology developments, so that personal data erased cannot be recovered and no personal data storage media would be discarded without going through a verification process to ensure that all personal data has been removed.

Recycling

The risk of data breach associated with recycling can sometimes be overlooked by data users. Recycling of print-outs containing personal data for other uses could result in such data being passed into the hands of unauthorised readers. Similarly, re-deploying computer equipment previously used for handling personal data without proper deletion could lead to personal data leakage. Data users must have clear policies and procedures in this respect so that employees understand the risks and know how to prevent such data leakage.

Engagement of Service Providers

In the case of outsourcing erasure work to a service provider (such as if specialised equipment is involved), the arrangement must be handled with care.

Both local and overseas experiences show that many data users, in outsourcing data erasure work to service providers, erroneously believes that they have also shifted their responsibilities or legal liabilities for safeguarding personal data privacy to the service providers. This results in a lack of monitoring of the work provided by service providers. In some cases, there is not even a written contract between the data user and service provider. **Section 65(2)** of the Ordinance clearly provides that any act done by an agent (e.g. a service provider) with the authority (whether express or implied) of another party shall be treated as an act done by that party.

Furthermore, both **DPP2(3)** and **DPP4(2)** require any data user engaging a service provider to process personal data to adopt contractual or other means to ensure that the service provider should comply with the relevant requirements under the Ordinance. At a minimum, data user should include in the service contract the requirements for erasure on (i) the security requirements relating to the transportation and handling of the personal data, (ii) the erasure standard and service level; (iii) the mechanism to ensure/confirm that all personal data is erased according to the agreed requirements; and (iv) the consequence of any non-compliance with the contract terms. For more information on the contract terms, please refer to Information Leaflet – Outsourcing the Processing of Personal Data to Data Processors[1] published by the Commissioner.

Employee Awareness

In this era of information technology, data users often allow their employees to access and download large amounts of personal data held by the data user. It is therefore very important to ensure that employees are aware of and adhere to the retention and erasure policies of an organisation. Sufficient training must be conducted regularly to raise awareness and make sure that all employees are playing their part effectively.

Destruction vs Anonymisation

Total erasure is not necessarily the only option for handling personal data no longer required for the purposes for which it was used. Data users may wish to retain part of the data for various reasons, such as for research and/or statistical purposes. If the personal data held is anonymised to the extent that the data user (or anyone else) will not be able to directly or indirectly identify the individuals concerned, the data is not considered to be personal data under the Ordinance.

[1] Available at www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf

Anonymising personal data means removing from the personal data any information from which an individual may be identified by anyone reading the record. Anonymisation also means that the data user is not in a position to re-establish the identity of any individual with its other existing or future information on the individual. Most importantly, data user should commit, by clear policy, that it does not and will not attempt to re-identify any individuals from anonymised data or to use the information or any individuals even if re-identification is possible.

Simply removing names, addresses or other such obvious identifiers (such as biometric data) may not be sufficient to make the data fully anonymous. When data contains complex or unique descriptions of individuals, it may be practicable for others to identify them even if the data does not contain any obvious identifiers. For example, if the data is related to a small group of people, such as a certain class of students, individuals may be reasonably ascertained if certain indirect identifiers, such as their area of residence, years attended, academic results on specific subjects/areas, are kept.

Furthermore, with the advancement of information technology, it may be possible for the data user or any third parties to ascertain or reasonably ascertain the identities of individuals using other publicly available information. To prevent this, data users must consider carefully whether or not to release the anonymised data to third-parties or the public.

Data users must realise that using anonymisation instead of erasure entails the risk that individuals may be re-identified from the data in the future. In this era of Big Data, there has been growing concern whether in the case of very large databases it will still be possible to genuinely and effectively anonymise individuals. Data users must make sure that the benefits of keeping anonymised data outweigh the potential risk that such data may be used to re-identify individuals, and the impact such re-identification would have on the individuals. For this reason, data users must review regularly whether anonymised data can be re-identified and take appropriate action to protect personal data.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Tel: (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