GUIDE TO DISPOSAL OF PERSONAL DATA ON PHYSICAL MEDIUM

Published 20 July 2016
Revised 20 January 2017

TABLE OF CONTENTS

PART 1: OVERVIEW

1 Introduction to Personal Data and Relevant Obligations

1.1 The use of individuals' personal data by organisations in Singapore is governed by the Personal Data Protection Act 2012 ("PDPA"). The Personal Data Protection Commission ("PDPC") was established to administer and enforce the PDPA and to promote awareness of protection of personal data in Singapore.

1.2 Personal data is defined in the PDPA as "*data, whether true or not, about an individual who can be identified a) from that data; or b) from that data and other information to which the organisation has or is likely to have access.*"

1.3 The term "personal data" ("PD") is not intended to be narrowly construed and covers all types of data from which an individual can be identified, regardless of whether such data is true or false or whether it is in electronic or other form. The most basic requirement for data to constitute personal data is that it is data about an individual. Data about an individual includes any data that relates to the individual, for example, full name, NRIC number, or a photographic image of the individual.

1.4 The PDPA defines 9 obligations for organisations in relation to personal data. Two of them are of particular relevance to this Guide:

1.5 The Protection Obligation under section 24 requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control.

1.6 The Retention Limitation Obligation under section 25 requires an organisation to cease retention of documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that there is no longer any legal or business purpose.

1.7 Organisations may refer to Chapter 17 (The Protection Obligation) and Chapter 18 (The Retention Limitation Obligation) of PDPC's *Advisory Guidelines on Key Concepts in the PDPA* for more information on these obligations.

2 Purpose and Scope of This Guide

2.1 This Guide is for persons responsible for data protection within an organisation, in particular for persons handling and disposing personal data stored or captured on a physical medium. In this Guide, 'physical medium' refers mainly to paper, but also to other read-only storage media such as CDs, DVDs, etc. For the purpose of this Guide, re-writeable media like hard discs, USB memory sticks, etc. would not be considered such 'physical media', as they allow for nearly unlimited overwriting of data, so that personal data may be disposed from these types of media without the need to dispose of the medium itself.

2.2 With a focus on personal data stored on paper, and shredding being used as a disposal method, this Guide seeks to provide:

- information on common topics related to disposal of personal data;
- good practices that organisations should undertake in disposal of personal data;
- examples of common mistakes that organisations and individuals may make in relation to the destruction of personal data; and
- information on considerations for out-sourcing disposal to third parties.

2.3 To meet the requirements of the PDPA, organisations should put in place:

- Documented policies and corresponding processes and procedures to protect data. The processes and procedures may involve external parties which are given access to personal data or copies of it. This Guide seeks to assist organisations in addressing such policies by providing a summary of information, issues, and best practices for disposal of personal data; and
- Schedules, which define the respective retention limitations for data held and controlled by the organisation (e.g. how long to keep records). It is not within the scope of this guide to cover the details on such schedules. However, organisations need to be aware that *untimely* or *unauthorised* disposal of personal data (whether by the organisation or a contracted third party) are important factors to consider beyond the methods applied during disposal, because they pose additional risks for the organisation.

2.4 While this Guide seeks to assist organisations in a general understanding of the issues around disposal of personal data, PDPC recognises that there is no 'one size fits all' solution. Each organisation should therefore adopt measures that are reasonable and appropriate for its circumstances. Some factors that organisations can take into account when deciding on the type of measures to adopt include:

- the type of personal data held by the organisation;
- the risk and impact to the individual should such personal data be accessed by unauthorised persons; and
- the form of the personal data (e.g. physical or electronic) in the organisation's possession.

2.5 Protection of personal data is implemented via security controls. They may come in the form of:

- physical controls, which limit the physical access to items;
- procedural or administrative controls, which consist of policies and procedures regulating the way of use; and
- technical controls, which are technological countermeasures.

2.6 Each of these control types contributes to the overall level of security. Strong controls in one area may compensate for weaknesses in other controls, or even make other controls redundant. Based on the organisation's risk management, the right type and level of controls, as well as the way they support each other, need to be chosen. In some cases, sector specific legal, regulatory, or compliance controls may apply and may have to be implemented as mandated. The type of control and its implementation will also depend on whether they are meant to be preventive, detective, corrective, or compensatory. In general, preventive controls should be used to protect personal data.

Example 1
Organisation X uses physical forms to collect personal data when new clients register for its services. These forms are stored in simple locked cabinets within a dedicated room. Access to the room is controlled by a PIN pad.
Organisation X relies primarily on physical control. The locked cabinets are in a restricted area with solid walls, whereby the access restriction compensates for the weakness of the simple lock. In the absence of the access restriction, a strong lock or metallic cabinet should be considered instead. Organisation X also uses administrative controls: a written rule that the PIN for accessing the room must not be communicated to others nor written down. Organisation X does not allow the PIN to be pasted beside the PIN pad.

2.7 This Guide does not offer an exhaustive list of disposal measures that organisations can adopt, nor does it replace or override any existing industry or sector standards,

nor is it a position statement or legal advice by PDPC. Organisations should also refer to other industry or professional literature on the topic. Organisations may also seek professional advice and services regarding disposal.

3 Definition of Terms

3.1 Total deletion or disposal of data in electronic (re-writable) medium is commonly referred to as '*sanitisation*' (e.g. purge or wipe files and unused space, degauss hard disks), whereas disposal of physical media is commonly referred to as '*destruction*'. Guidelines and tools for sanitisation are commonly available (e.g. PDPC's *Guide to Securing Personal Data in Electronic Medium*); some sanitisation methods permit re-using the medium whereas others may render the medium unusable.

3.2 This Guide focuses on the aspect of destruction, mainly addressing paper (documents, photos, posters, etc.) storing personal data; destruction makes the medium non-reusable. While some electronic media like USB sticks and hard disks may allow for sanitisation to some degree (basically by overwriting the data), other media do not support overwriting (e.g. write-once or read-only CDs, DVDs, etc.) and therefore require physical destruction. Similar principles as described in this Guide for paper medium may apply to electronic media that do not support overwriting, be it because they don't support sanitisation or because physical destruction in addition to 'logical' or 'electronic' sanitisation is needed.

3.3 As such, there are two methods for the disposal of personal data: a) destroy the medium carrying the data; or b) dispose only the data itself. By destroying the medium, the data is rendered inaccessible. For some storage media, it is possible to securely erase the data without destroying the storage medium, but specialised software or tools may be needed. Destruction of medium is generally applied to non-electronic, single-use storage media, whereas standalone data erasure is associated with electronic media. The effect of the disposal method must be such that the data cannot be recovered (partially or fully) regardless of whichever method is used.

> *Example 2*
> Personal data stored on paper can be disposed by burning the paper. Unless the burning is incomplete, neither the paper nor the data on the paper can be recovered. Personal data stored on hard disc can be disposed by erasing it with a specialised software tool. The tool will only purge the data, while the hard disc remains intact and can be reused. Proper purging will ensure that the data is indeed

removed; a simple deletion of data by dragging the file into the "trash bin" icon on the computer is not sufficient, as the data may still be recoverable.

PART 2: PHYSICAL DISPOSAL MEASURES

4 Data Life Cycle

4.1 Data Life Cycle refers to the stages and transformations, which data undergoes from collection (it is rare that personal data is newly created) to destruction. A typical life cycle comprises the following stages:

4.2 During the entire life cycle, personal data must be protected. This does not apply only to the original data set, but also to any copies, print outs, and transformations (with the exception of anonymisation). While copies of personal data on paper (especially in large volumes) are less easy to distribute than their electronic counterparts, they still need to be taken into consideration. Disposal of personal data is therefore not just about the main document but about each and every copy of such document when the data is not needed anymore. Essentially, whenever you create a copy, that copy would have a separate and new data life cycle.

Example 3
Organisation X collects personal data via a form during a marketing campaign. Afterwards the data is digitised for further processing, and soon the forms are not required anymore. Two life cycles overlap here. The life cycle of the data on the form has passed the 'collection' stage and is at the use and replication stage when the digitised copy starts its own life cycle through the digitisation. While the life cycle for the digitised data remains active and stays for a longer period in the usage stage, the form has fulfilled its purpose and is ready to end its life cycle through the disposal stage, e.g. through shredding, skipping the maintenance and archival stage.

4.3 Disposal applies to any type of medium that data is stored on. For example, such data may first be created online and subsequently printed out, copied on CD's, etc. Many other copies may also be created, some of which may be short lived, such as

handwritten notes, or persist longer, as in print-out for meetings. Just like protecting its confidential information, an organisation must hold and dispose of personal data in a secure manner.

5 Importance of Disposal

5.1 Disposal in this Guide refers to the overall process of transforming or destroying information in a way that renders it unreadable (for paper records) or irretrievable (for electronic records). Disposal should not to be taken lightly; it needs to be well managed and controlled throughout the entire data life cycle.

5.2 It is important to note that the Protection Obligation under the PDPA does not end with personal data simply being discarded in the (physical or electronic) trash bin. Incomplete disposal can lead to data breaches, such as:

- Deleted electronic files or improperly shredded paper may be restored (in full or partially); and
- Uncontrolled disposal of paper without destruction may lead to recovery of documents through 'dumpster diving' (e.g. sifting through physical waste or recycling containers for items that have been discarded, but are still of value or covered by regulation).
- Even for a medium, where sanitisation is possible, due to technological issues and advances in sophistication of hackers and attack methods, the (additional) destruction of the medium itself may be required where such a medium holds more sensitive or high volume of personal data.

6 Main Approaches for Paper Disposal

6.1 For personal data stored on physical media and in paper form, PDPC's *Advisory Guidelines on the Key Concepts in the PDPA*, advises organisations to ensure proper disposal of the documents that are no longer needed, through shredding or other appropriate means.

6.2 For personal data stored on paper, proper disposal or destruction usually refers to putting the paper through one or more of the following processes[1]:

[1] For pulping and incineration, please also refer to Part 4 of this document which covers out-sourcing of disposal to third party service providers, in particular paragraph 10.3.

- *Incineration* (or burning): reduces paper to ashes;
- *Shredding*: cuts paper in a way that makes it reasonably difficult, or even impossible, to reassemble the pieces in order to reconstruct (a substantial part of) the information, but allows for the paper to be recycled as long as the pieces are not too small; or
- *Pulping:* paper is mixed with water and chemicals to break down the paper fibres before it is processed into recycled paper.

6.3 Shredding (cf. section 7 for more details) is commonly used by organisations as it is considered a fast, safe, and cost-effective method. It is also considered sufficiently secure for a wide range of documents, where 'reasonable difficulty' in reconstructing the document is required. After shredding, the shredded paper can be recycled. From an environmental perspective, shredding followed by recycling of paper is preferred over incineration.

6.4 Most disposal methods can be carried out in-house by the organisation itself or by an external third party service provider. The choice typically depends on the type, amount and frequency of the disposal exercise. Organisations should be aware that outsourcing the disposal of personal data does not imply that the organisation would not be accountable anymore for the personal data once it hands over the media containing the personal data to an external third party. The organisation must still ensure that the external processing is still in compliance with the Protection Obligation under the PDPA. Outsourcing arrangements should take this into consideration (cf. Part 4 for more details).

7 Paper Shredding

7.1 For documents that contain personal data, leaving them unattended while they await being discarded or destroyed may provide opportunities for a third party to gain access to the information, e.g. leaving them at the rear entrance of the office or at the bottom of the building, for collection by the paper disposal vendor. Likewise, tearing such document into halves or quarters and then dropping it into the waste bin does not destroy the data on the paper. Reusing paper documents that are scheduled for shredding can increase the risk of personal data on these documents being compromised.

7.2 Depending on the category of information stored on the document, different shredder specifications may be required to properly shred the paper. For example, a shredder which only cuts the paper into strips, a so-called *straight-cut* shredder, may still allow

a third party to reassemble the strips into the original document. If the unauthorised disclosure of the information contained on the paper document could result in significant impact to an individual (e.g. the document contains healthcare data or financial information about the individual), organisations may wish to consider using a shredder that cuts the paper into separate small pieces, which make it more difficult to reassemble. These features on shredders are commonly known as *cross-cutting* capability, where the paper documents are sliced in at least two different directions to create individual pieces. *Confetti* shredders achieve the same outcome of destroying information on paper documents and they also crumple the cross-cut pieces.

7.3 Paper shredders are typically categorised by levels, which indicate a suitability of the shredder for certain types of information, e.g. general, internal, confidential, sensitive etc. Higher levels indicate a more thorough damage to the paper, typically expressed in the shape and size of the resulting pieces (also called "remnants"). For example, the DIN 66399 standard[2] defines 7 levels of security for different types of media. Although this standard may not have official status in all jurisdictions, it is internationally referenced. When a shredder does not indicate any DIN level, the organisation may use the resultant piece size as a reference to compare with the DIN standard, based on the material shredded.

7.4 The 7 levels for paper are:

Level	Paper
P-1	Strip width max. 12 mm
P-2	Strip width max. 6 mm
P-3	Particle size max. 320 mm^2
P-4	Particle size max. 160 mm^2
P-5	Particle size max. 30 mm^2
P-6	Particle size max. 10 mm^2
P-7	Particle size max. 5 mm^2

7.5 For personal data on paper[3] the DIN 66399 standard recommends the use of at least a level P-3 cross cut shredder, which shreds paper into particle size of maximum 320mm^2. Disposal of personal data on paper documents is a process which only ends when the paper document is fully destroyed or properly shredded.

[2] Older shredding devices may use the previous DIN 32757 standard.

[3] The DIN standard states different particle sizes for different media. The type of media is indicated in the prefix of the level: "P" stands for paper, "O" stands for optical (like DVD, CD), etc.

PART 3: SHREDDING ISSUES AND PRACTICES

8 Typical Disposal Mistakes and Issues

8.1 A complete data set is often considered more important and thus extra care is more likely to be taken during disposal. However, it is a common mistake to neglect personal data where:

- It is only part of a whole data set (e.g. just the first page of a completed form);
- There are mistakes in some fields (therefore data is deemed inaccurate); or
- It contains printing errors (e.g. letter to customer printed with errors in the title or date).

8.2 As mentioned in the introductory chapter, personal data is any data which, on its own or with other information, allows an individual to be identified. Such data may not necessarily be true or up-to-date or complete, so long as it allows for identification of an individual.

8.3 Also, after an organisation decides to dispose of paper documents, they are often perceived as 'valueless' and 'unimportant'. This perception can lead to unsecured treatment or storage of documents, e.g. while they are pending actual destruction. As a result, these documents may end up being stored at poorly supervised and less frequented places, which increase the risk of misuse or misappropriation.

8.4 Typical problems involving printouts containing personal data include:

- Paper recycling is encouraged by the organisation, and without rules in place, paper meant for shredding is recycled without first destroying it;
- Staff is not sufficiently trained or aware about protecting personal data even when it is 'not used' anymore in the current form or has become obsolete;
- Staff not checking whether the reverse page of waste/recycled paper contains any personal data and simply discard or leave it unattended;
- Containers meant to collect confidential documents are not sufficiently marked and differentiated from common collection containers, e.g. for recycling; or
- Confidential documents are left in an unsecured area.

8.5 Although papers and documents may be centrally collected for disposal, there are additional steps involved between the collection itself and the actual disposal, which can lead to unauthorised access, such as:

- Documents intended for shredding are stored in the same place as documents meant for plain recycling; and
- Documents are not protected between their release for disposal and their actual destruction, e.g. they may be simply kept in unsecured boxes or containers, which may become targets for dumpster diving or theft.

8.6 Apart from issues pertaining to the paper and the information on the paper, there are also common problems around the shredders, such as:

- No easy access to the shredder, or use of shredder causes noise issues for nearby staff;
- Shredder wastebaskets are not regularly cleared;
- Improper use of shredders, leading to frequent breakdowns; or
- Shredders are slow, requiring users to spend significant time to shred.

9 Good Practices

9.1 To address typical issues and problems in destroying paper documents, the following best practices should be considered for implementation:

- When in doubt whether the paper document contains personal data, shred the document; and
- Encourage staff to shred paper documents containing personal data regularly to cultivate the habit. Shredded paper can still be sent for recycling, encouraging environmental sustainability.

9.2 Organisations need to keep in mind that everyone handling paper documents are to be briefed on the right way to deal with such documents from creation to disposal, whether they are permanent staff, contract staff, third party provider, volunteer, intern, etc. This includes cleaners who help clear the wastepaper in offices. Important points to mention in the briefing includes:

- Waste paper from allocated areas inside the office (e.g. confidential material boxes) should not be brought to non-designated areas for disposal or handed over to anyone other than authorised parties; and

- Waste paper that contain personal data of individuals should not be retained or used for other purposes, such as scrap paper for wrapping or writing, or to layer the bottom of waste baskets.

Ad-hoc checks should be conducted by the organisation to ensure compliance.

> *Example 4*
> Organisation X contracted a third party cleaning service provider Y for the office. Provider Y deploys its cleaning staff A to organisation X. On the first day, cleaner A is given a tour through the office by employee B. When they reach a box marked "Confidential", employee B gives cleaner A specific instruction that this box must be handed over to the designated disposal service provider Z every Monday morning. Employee B emphasises that the papers inside the box are not to be taken out at any point in time. Employee B illustrates this point by giving the example that these boxes cannot be given to any 'garang guni' man or another recycling organisation without the approval of the Organisation.

9.3 To assist organisations in assessing their practices in disposal of personal data on documents, a checklist of good practices is available at **Annex A.**

PART 4: THIRD PARTY SERVICE PROVIDERS

10 Considerations When Outsourcing Disposal of Paper Documents and Other Physical Media

10.1 When disposal of paper documents is outsourced, the accountability and responsibility to ensure that the personal data on such paper documents are destroyed remains with the organisation. Therefore, where disposal is outsourced, the organisation should ensure that contracts with third party service providers contain the necessary terms and conditions to comply with the obligations under the PDPA.

10.2 This includes having such third party service providers take reasonable measures to protect the personal data on the paper from disclosure to unauthorised parties during the entire disposal process. To do so, organisations would need to understand how these third party service providers dispose of the paper, including the supply chain arrangements. For example, does the third party itself perform collection and disposal, or are sub-contractors involved in collection or disposal? Or what measures does the third party have in place to ensure that the documents containing personal data transported by its trucks are not accessed without proper authorisation between the

place of collection and the place of disposal? In particular, when the paper is not shredded before being collected, or when bulk shredding service is provided by yet another third party, the organisation needs to be aware if the processing is done in Singapore or overseas.

10.3 Where the paper (or physical medium) containing personal data is transferred overseas to be destroyed or recycled, the organisation will need to further ensure that such transfer complies with the Transfer Limitation Obligation[4] under the PDPA. This may apply in particular to pulping and incineration, as these types of disposal may not be available or are limited in Singapore. Organisations may therefore wish to check with their disposal vendors if their paper (or physical medium) containing personal data are sent overseas to be recycled or incinerated.

10.4 Summary of points to consider when outsourcing disposal:

- Assess the suitability of the services for the kind and volume for disposal; for mass disposal of documents in files and with clips etc., ensure that the disposal service permits metal or plastic pieces;
- Assess the service provider's overall processes and protection during transport, storage, and actual destruction; it may be more difficult to assess cases where only the collection is done in Singapore, but actual destruction occurs at an overseas location;
- Assess whether containers are locked or secured during transit, whether policies for accident and incident reporting are in place, and whether the shredding/incineration/pulping facility has physical security in place;
- Keep records of collection and destruction confirmation. Some service providers may be certified or accredited, and may be able to provide a formal certificate of destruction; otherwise maintain internal records when these matters have been sent for disposal;
- Collection (or handover) of waste items (e.g. paper documents) should be supervised and documented; the waste items should not be stored unsecured for easy collection by the outsourced party;

[4] Section 26 of the PDPA limits the ability of an organisation to transfer personal data outside Singapore. In particular, section 26(1) provides that an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA. Organisations may refer to Chapter 19 (The Transfer Limitation Obligation) of the PDPC's *Advisory Guidelines on Key Concepts in the PDPA* for more information.

- Intermediate storage locations should be secured; e.g. due to over-capacity, items might need to be temporarily stored before they are destroyed; and
- An officer of an appropriate level should witness the actual destruction, or even follow the third party's disposal vehicle, especially when sensitive personal data is involved.

END OF DOCUMENT

Annex A: Consolidated Checklist of Good Practices

Checklist of Good Practices		
1	If your organisation recycles used paper, are the staff reminded to check whether there is personal data left on the paper before sending for recycling? (If there is, those recycled papers should be disposed of properly)	☐
2	Are your staff aware that they should check if wastepaper (e.g. extra copies, wrong copies, unused copies) contains personal data and how to dispose them properly?	☐
3	Does your organisation leave wastepaper outside its premises unattended? If so, does your organisation first check that there are no confidential documents or documents containing personal data of individuals?	☐
4	Is the shredding machine regularly cleared and serviced?	☐
5	If your organisation has outsourced its document disposal, was there a review on how the third party disposes of the paper and whether such practices comply with the PDPA?	☐
6	Has your organisation nominated a data protection officer, who is overall in charge of personal data protection, and to whom staff can refer to when they need further clarification on personal data protection and disposal?	☐
7	Does your organisation have disposal policies in place, which determine how the different data must be disposed of, and are they regularly reviewed?	☐
8	Does your organisation have retention policies in place, which determine when certain types of data should be disposed of or how long they should be archived for business reasons?	☐

BROUGHT TO YOU BY