GUIDE TO SECURING PERSONAL DATA IN ELECTRONIC MEDIUM

Published 08 May 2015
Revised 20 January 2017

TABLE OF CONTENTS

PART 1: OVERVIEW

1 Introduction

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

2 Purpose and Scope of This Guide

2.1 The Protection Obligation under section 24 of the PDPA requires organisations to make reasonable security arrangement to protect personal data in their possession or under their control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Organisations may also refer to Chapter 17 (The Protection Obligation) of the PDPC's Advisory Guidelines on Key Concepts in the PDPA for more information.

2.2 This Guide is for persons who are responsible for data protection within an organisation and also persons who supervise or work with infocommunication technology ("**ICT**") systems and processes. Some ICT knowledge will be required to understand the terminology and concepts used.

2.3 This Guide seeks to provide:

- information on common topics related to security and protection of personal data stored in electronic medium (or "**electronic personal data**");
- good practices that organisations should undertake to protect electronic personal data; and
- enhanced practices that organisations may consider adopting to further improve protection of electronic personal data.

Note: In this Guide, the ICT security measures listed in each section are differentiated as follows:

Good practices are listed in tables with a blue background like this
Enhanced practices are listed in tables with a white background like this

2.4 While this Guide seeks to assist organisations in protecting electronic personal data, the Commission recognises that there is no 'one size fits all' solution for organisations. Each organisation should therefore adopt security measures that are reasonable and appropriate for their circumstances. Some factors that organisations can take into account when deciding on the type of security 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 and used by unauthorised persons; and
- the form of the personal data (e.g. physical or electronic) in the organisation's possession.

2.5 This Guide does not offer an exhaustive list of ICT security measures that organisations can adopt to protect electronic personal data, nor does it replace or override any existing industry or sector ICT security standards. Organisations should also refer to other industry or professional literature on the topic. Organisations may also seek professional advice and services regarding ICT security, where necessary.

PART 2: ADOPTING ICT SECURITY MEASURES

3 ICT Security and Data Breach Risks Involving Personal Data

3.1 Storing of personal data on computers or making data available on the Internet offers many advantages over non-electronic methods. However, organisations should be aware of potential security and data breach risks as well as issues that may arise from them. Reasonable security arrangements should therefore be made to reduce security risks and the incidence of data breaches[1].

3.2 Security incidents and data breaches involving electronic personal data can be caused by a variety of means. Some examples of these causes are:

- hacking or other unauthorised access of databases;
- physical attacks such as use of skimming devices on Automated Teller Machine ("**ATM**");
- malware or hostile programs such as computer viruses and spyware;
- social engineering, such as phishing scams and the circulation of malware-laden email attachments;
- unauthorised access or misuse of personal data by employees or vendors;

[1] Please refer to the PDPC's *Guide to Managing Data Breaches* for more information.

- loss or theft of electronic devices or portable storage devices containing personal data;
- fault or weakness in a system's or device's program code causing it to reveal personal data to incorrect parties, such as a bug in an online portal allowing someone to access another person's data;
- compromised network devices;
- compromised point of sales ("**POS**") systems;
- not disposing of electronic personal data properly; and
- unintended disclosure of personal data to another individual other than the intended recipient, such as emailing to the wrong recipient.

4 Governance

4.1 Managing ICT security and risks related to data breaches requires good governance. There are four components of governance that organisations should take into consideration: a) Accountability; b) Standard, policies, and procedures; c) Risk management; and d) Classification and tracking.

Table 1: Governance	
Clear accountability	
Good practices	
a	Provide clear direction on ICT security goals and policies for personal data protection within the organisation.
b	Identify and empower the person(s) accountable for personal data protection within the organisation.
Standards, policies and procedures	
Good practices	
c	Establish and enforce ICT security policies, standards and procedures.
d	Review and update ICT security policies, standards and procedures periodically to ensure relevance.
e	Establish end user policies to prevent misuse of ICT systems.
Risk management	
Good practices	
f	Institute a risk management framework to identify the security threats to the protection of personal data, assess the risks involved and determine the controls to remove or reduce them.

g	Assess the effectiveness of the risk mitigation controls periodically.
h	Assess the security risks involved in out-sourcing or engaging external parties for ICT services and mitigate them.
Classification and tracking	
Good practices	
i	Classify and manage the personal data by considering the potential damage (e.g. reputational or financial) to the individuals involved should the data be compromised.
j	Conduct periodic checks for personal data stored in ICT systems. For personal data that is not required in any form anymore, securely dispose the data (refer to section 8). If there is a need to retain the data but not in identifiable form, e.g. for performing data analytics, consider anonymising[2] the data.
k	Conduct physical asset inventory checks regularly to ensure all computers and other electronic devices (e.g. portable hard drive, printer, fax machine etc) used to store or process personal data are accounted for.

5 Security Awareness

5.1 Increasing awareness of ICT security threats and protection measures among employees helps to reduce the risk of data breaches through system misuse or mistakes. An example of awareness among employees is to be cautious about phishing or other forms of social engineering. They should also be made aware of the security policies and standards relevant to their work.

5.2 Software developers and other ICT personnel should also be aware of current and emerging ICT security threats, in order to design and maintain ICT systems capable of protecting personal data stored.

Table 2: Security Awareness	
Good practices	
a	Educate employees on ICT security threats and protection measures for personal data. This includes the organisation's ICT security policies, standards and procedures.
b	Keep ICT security awareness training for employees updated and conduct such training regularly.

[2] Refer to the PDPC's Advisory Guidelines on Anonymisation for more information.

6 Compliance, Testing and Audits

6.1 Holding regular assurance checks help organisations ensure that ICT security controls developed and configured for the protection of personal data are properly implemented and practised.

Table 3: Compliance, Testing and Audits	
Good practices	
a	Conduct regular ICT security audits, scans and tests to detect vulnerabilities and non-compliance with organisational standards.
b	Apply prompt remedial actions to detect security vulnerabilities and any non-compliance with established policies and procedures.
c	Implement measures to ensure ICT system logs are reviewed regularly for security violations and possible breaches.

7 Authentication, Authorisation and Passwords

7.1 Authentication and authorisation processes in ICT systems are commonly used to ensure that information is accessed by the intended persons performing required activities only.

7.2 Authentication is the process of verifying the identity of a user. User Identifiers ("**IDs**") and passwords are commonly used to identify and authenticate authorised users.

7.3 The strength of authentication, such as password requirements or other mechanisms for access to personal data, should depend on the potential damage to the individual, such as potential damage to reputation or finances, if such personal data is compromised. Password policies should also require changes to passwords periodically. There should be mechanisms in an organisation's ICT systems to enforce the policy in terms of password selection and change.

7.4 More secure authentication methods include two-factor or multi-factor authentication. These involve the use of a combination of information that the user knows, such as a password or PIN, and an object that only the user possesses, such as a digital key, token or smart card, or a unique physical trait, such as the use of fingerprints in biometric technology. The use of multi-factor authentication increases confidence in the identity of the user accessing the system.

Example 1

Organisation X has two internal IT systems containing personal data: (i) System A, which is used to manage customer contact details, and (ii) System B, which contains the financial statuses and transaction details of customers.

For System A, Organisation X implements user authentication with a minimum password length of 8 characters. For System B, password requirements are the same as for System A, and two-factor authentication is also implemented. In addition to the password, the user has to key in a one-time password sent to the user's mobile phone, to access System B.

Example 2

Organisation Y has an IT system which requires ordinary user accounts to have a password change every 90 days. Administrator accounts are required to have a password change every 60 days.

Table 4: Authentication	
Good practices	
a	Determine a suitable authentication method, single factor or multi-factor, for accessing personal data based on the risk of damage to the individual in case of a data breach.
b	Determine a suitable maximum number of attempts allowed for a user to authenticate his or her identity based on the type of data to be accessed.
c	Implement account lockout when the maximum number of attempts is reached, to prevent dictionary or brute-force attacks, which refer to methods of systematically checking all possible keys or passwords until the correct one is found.
d	Password used for authentication has a length of at least 8 characters containing at least 1 alphabetical character and 1 numeric character.
e	When password used for authentication is typed in, it is to be hidden under placeholder characters such as asterisks or dots.
f	Password used for authentication is encrypted during transmission and also encrypted or hashed in storage. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.

g	Users are required to change their passwords regularly. The frequency should be based on the risk of damage to the individual if the data is compromised.
h	Change default passwords to strong passwords at the earliest possible opportunity.
Enhanced practices	
i	Assign unique and distinct user ID to individual users.
j	Encourage users not to use passwords that can be easily deduced, such as their birth date or name.
k	Users to change system-generated password upon first login.
l	Discourage users from using the same password across different systems or applications.
m	The same password is not allowed to be reused within the last 3 changes.
n	Password used comprises both lowercase and uppercase characters.
o	Password used comprises special characters such as '!', '&', etc.

7.5 Authorisation is the process of verifying whether a user has the rights to access the resources being requested, such as access to a network or database.

7.6 Authorisation usually happens after authentication.

Example 3

Organisation Y has a centralised IT system for Human Resource ("**HR**") and marketing purposes. Employee X, a marketing staff, should only have access to resources such as personal data, graphs, etc. of the system that are relevant to his role. The system administrator should not allow Employee X to access the system's HR records or functions.

Table 5: Authorisation	
Good practices	
a	Implement authorisation mechanisms and processes to check if the person accessing the system has appropriate access rights to data requested within the system.
b	Define user roles or groups for systems that enable access to personal data. Access rights for each user role or group should be clearly defined and reviewed regularly.

c	Grant a user only the necessary access rights to personal data within systems to fulfil their role or function.
d	Track and review usage of accounts and their associated access rights regularly. Remove or change access rights for unused or obsolete accounts promptly.
e	Log all successful and failed access to systems to help detect unauthorised attempts to gain access to them.

8 Destruction of Electronic Personal Data

8.1 Organisations should dispose of or destroy personal data when it is no longer necessary to retain it in any form, for any business or legal purpose. Organisations should ensure that it is done in a manner that the data cannot be recovered or disclosed. Personal data can also be anonymised[3] to prevent identification of individuals.

8.2 Data is often stored on electronic storage media. This includes magnetic storage media such as hard disks or floppy disks, solid state drives ("**SSD**"), Universal Serial Bus ("**USB**") flash drives and optical storage media such as Compact Discs ("**CDs**") or Digital Versatile Discs ("**DVDs**").

8.3 As electronic assets (e.g. computers) become outdated or replaced, they are often sold or disposed of by organisations through various means, including returning the equipment to the vendor, selling to a third party or throwing them away. The electronic storage media in the assets may still contain personal data and there is a risk of unauthorised disclosure of such data when the media are disposed without proper care.

8.4 It must be noted that data stored on electronic storage media are generally not completely erased through the common 'delete', 'clear recycle bin' and even 'format' commands used in standard operating systems. Most operating systems do not fully delete the actual file in the storage media. Instead, the 'deleted' file is simply removed or delinked from the user's view, but the data is still intact within the systems until overwritten by new files. Commonly available software can recover 'deleted' files, which may contain personal data stored on such devices.

8.5 Software solutions are available to securely erase data stored on magnetic storage media by overwriting selected files or the entire storage drive. The number of passes, or the number of times that overwriting is done, can usually be specified. A greater number of passes increases the certainty that the original data would be overwritten

[3] Refer to the PDPC's Advisory Guidelines on Anonymisation for more information.

and more unlikely to be recovered. Specialised hardware appliances are also available to securely erase data from electronic storage media.

8.6 Some overwriting standards to securely delete data are available. These include the U.S. Department of Defence Sanitising (DOD 5220.22-M) standards and NIST SP-800-88 – a special publication by the US-based National Institute of Standards and Technology.

8.7 However, simple overwriting of files alone may not be sufficient for all types of storage media. Another proven method for destroying magnetic storage media is degaussing – the removal of magnetic fields from an item. Degaussing is performed by a degausser machine which produces a strong electromagnetic field to destroy magnetically recorded data. Note that the process of degaussing may render magnetic storage media unusable.

8.8 Physical methods may also be employed to destroy disk drives. These include drilling through hard disks. Some knowledge is required before using such methods, such as knowing which parts of a hard disk should be drilled through and how many holes should be drilled in order for the drive to be securely destroyed. Other physical destruction methods include crushing and shredding the disk drive[4].

Table 6: Destruction of Data	
Good practices	
a	Identify storage media to be destroyed or sold, and put in place a process to track whether personal data had been stored on them.
b	Perform secure deletion, erasure or destruction of electronic personal information on storage media before redeploying, exchanging or disposing of the media.
c	Perform physical or other known methods of destruction of storage media such as degaussing and incinerating when secure deletion, erasure or deletion of personal data stored on the media is not possible. This may be the case with faulty storage media.

9 Computer Networks

9.1 Computer networks allow communication between computers and devices that are connected to them. Internal corporate computer networks may be connected to external networks, such as the Internet. It is important for an organisation to ensure

[4] Some storage media (like read-only DVDs) may not allow for secure deletion via overwriting at all; for these physical destruction is the only option. For added guidance see PDPC's *Guide to Disposal of Personal Data on Physical Medium*.

that its corporate computer networks are secure. Vulnerabilities in the network may allow cyber intrusion, which may lead to theft or unauthorised use of electronic personal data. Defences that may be used to improve the security of networks include:

- Intrusion prevention systems ("**IPS**") - a device or software application that monitors network or system activities and prevents malicious activities or policy violations;
- Intrusion detection systems ("**IDS**") – a network security appliance that monitors network and system activities for malicious activities and may raise alerts upon detecting unusual activities;
- Security devices that prevent the unauthorised transfer of data out from a computer or network;
- Firewalls; and
- Web proxies, anti-virus and anti-spyware software.

9.2 Wireless local area networks ("**WLANs**"), also commonly referred to as WiFi networks, which link two or more devices wirelessly in a limited area, are common in many organisations. Wireless networks offer advantages such as easier deployment and mobility within the area to users, as compared to wired networks. However, wireless networks are also generally regarded as more vulnerable, because a cyber-attacker does not need to be physically connected to the network. Traffic from wireless networks may also be more easily intercepted through the airwaves.

Table 7: Computer Network Security	
Good practices	
a	Equip networks with defence devices or software.
b	Review configuration settings regularly to ensure they correspond to current requirements.
c	Design and implement the internal network with multi-tier or network zones, segregating the internal network according to function, physical location, access type etc.
Enhanced practices	
d	Apply secure connection technologies or protocols when transmitting electronic personal data, such as over a computer network or from one network to another.
e	Disable unused network ports.
f	Monitor LAN/WiFi regularly and remove unauthorised clients and WiFi access points.

g	Use two-factor authentication and strong encryption for remote access. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.
h	Use network proxies to restrict employee access to known malicious websites.
i	Disallow remote network administration.

10 Personal Computers and Other Computing Devices

10.1 Personal computers and other computing devices (collectively referred to here as "computers") are commonly used by employees for communication and other work purposes. These computers are commonly installed with software such as email, word processing, spreadsheet and presentation tools. Often, in the course of work, some amount of personal data may be stored on the computer's local storage, like its hard disk.

10.2 A basic way to reduce unauthorised access to computers is to turn on password checking features. Examples are keying in of password during boot-up, requiring login to the operating system, locking the screen after a period of inactivity and so on.

10.3 Encrypting the data on a computer's local storage provides another layer of protection. Various types of data encryption are available. These include full disk encryption, virtual disk encryption, volume encryption, file/folder encryption and application level encryption.

10.4 There are various algorithms that may be used for encryption, and the strength of the encryption generally depends on the algorithm used, as well as the length of the encryption key. Typically, the longer the encryption key length, the more secure the encryption. It is also important to manage and protect the encryption keys, in particular, to keep the encryption keys secure and separate from the encrypted data.

10.5 It should be noted that data stored in encrypted form does not protect against situations where the data is in use. E.g. for full disk encryption, while the computer is switched on, the encryption of the drive is transparent to the user. Hence, a cyber-attacker could still gain access to encrypted data stored on the computer while it is switched on. A screen lock would offer some protection in this situation if the computer were to remain switched on. On the other hand, for file-based encryption, the file would remain protected until the user explicitly decrypts the file with the correct password.

10.6 Users should be given appropriate account types. Users who do not need administrator accounts should not be given one, as these administrator accounts have the potential

to do more harm if compromised, due to elevated privileges. Similarly, administrators should only use administrator accounts when needed for the task, and use a second, 'normal' user account for tasks which do not need administrative rights.

10.7 Shared computers are sometimes used, e.g. by customers filling up online forms or employees registering during an organisation event. Additional precautions can be taken to restrict access to personal data, e.g. by turning off "auto-complete" and turning on "private" browsing mode.

10.8 In general, software that is not required for work or other official use should not be installed. The less software is installed on a computer, the lower is the likelihood that vulnerabilities are present. This is especially true for software that is obsolete and/or unsupported.

Table 8: Security of Personal Computers & Other Computing Devices	
Good practices	
a	Protect computers by using password functions.
b	Install anti-malware software such as anti-virus, anti-spyware, and software-based firewall on computers. Keep them updated and perform scans regularly.
c	Encrypt sensitive personal data, which has a higher risk of adversely affecting the individual should it be compromised. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.
d	Prevent unauthorised personnel from viewing the screens of personal computers easily, such as by using privacy filters, or through positioning of the personal computer.
e	Enforce password policy as indicated in Table 4.
f	Implement additional controls for shared computers to prevent access to personal data, e.g. those keyed in by another user.
Enhanced practices	
g	Disallow anonymous or guest logins.
h	Disallow non-administrator users from booting up a computer using external or removable storage media.
i	Disallow non-administrator employees from installing software or changing security settings, except on a need-to basis. Keep administrator accounts for administrator use only.

j	Remove unused software and turn off unnecessary services from computers.
k	Install or activate Application Control solutions.

11 Portable Computing Devices & Removable Storage Media

11.1 Common portable computing devices used in organisations include notebook computers, tablets and mobile phones. Removable storage media such as USB hard disks, backup-tapes, USB flash or thumb drives, as well as memory cards are also commonly used.

11.2 Portable computing devices and removable storage media are generally considered more susceptible to being misplaced or stolen as compared to desktop personal computers. Additional security measures should be taken to protect these devices and media. (*Note: Section 10 would also apply to portable computing devices.*)

11.3 Security measures taken to protect portable computing devices should apply whether the devices are issued by organisations or owned by employees (e.g. Bring Your Own Device or BYOD).

11.4 Portable computing devices are often connected to the Internet via less secure WiFi access points at external or public places, e.g. at conference venues or an overseas hotels. An additional risk arises in such situations from spoofed access points. A cyber attacker could set up a fake access point with a Service Set Identifier (SSID) that looks very similar to the venue's official SSID. This could trick users to connect to it and potentially allow personal data to be intercepted by the cyber attacker.

Example 4

Organisation X issues its consultants with tablets. The consultants often meet clients out of office. The tablets are installed with customised software that allows the consultants to service clients. Personal data pertaining to the clients are stored centrally at corporate servers, and access to the personal data through the tablets requires two-factor authentication.

Upon logging into the tablet and its customised software, the tablet only provides access to personal information of clients who are served by the consultant instead of the entire database. The tablets are configured to automatically screen lock upon 60 seconds of inactivity, whereby user authentication is required to unlock the device. The consultants

also observe a policy of not leaving the tablets unattended for any amount of time when in public areas.

Table 9: Portable Computing & Removable Storage Media Security	
Good practices	
a	Identify and take stock of the portable computing devices and removable storage media that may be used by your organisation to store personal data.
b	Minimise storage of personal data on portable computing devices and removable storage media. Remove personal data that is no longer required as soon as possible. (For additional information, refer to Section 8)
c	Secure portable computing devices and removable storage media when not in use. This can be done by keeping them under lock and key, attaching them to a fixture by a security cable, hand-carrying, and not leaving them unattended.
d	Configure portable computing devices to automatically lock upon a period of inactivity, whereby a password is required to resume usage.
e	Assess the applications that users can install and establish a policy for the use and tracking of the organisation's portable computing devices and removable storage media.
Enhanced practices	
f	Install and activate remote device locking and wiping features, which allow the portable computing devices to be locked and local data erased from any location in the event of theft or loss of device.
g	Turn off wireless communication features such as Wi-Fi and Bluetooth when these are not in use.
h	Connect to external WiFi access points carefully and secure communications, e.g. by using Virtual Private Networks (VPN).

12 Printers, Copiers, Scanners and Fax Machines

12.1 Printers, copiers, scanners and fax machines are found in almost every office. These machines are often connected to the office computer network. Many offices are also equipped with multi-function machines that can print, copy and fax. As the same security measures apply to printers, copiers, scanners, fax machines and similar multi-function machines, this Guide shall refer to all these machines collectively as multi-function printers ("**MFPs**") for ease of reference.

12.2 Modern MFPs are often equipped with a storage device which contains a digital copy of the documents sent for print and any associated metadata, such as the document title and document owner.

12.3 MFPs may be a source for accidental disclosure of personal data. Some of the ways in which personal data might be disclosed when using MFPs are:

- data intercepted while being sent to the MFP;
- unattended hardcopy printouts in printer trays viewed or taken by unintended persons; or
- data extracted from the MFP's local storage device.

12.4 To reduce the risk of data interception while data is being sent to an MFP, or when a scanned document is sent to the user's computing device after a scan, a secure internal corporate network is required (refer to section 9 on Computer Networks). To address the risk of printouts being intercepted, some MFPs are equipped with a secure print (also known as pull print) feature, whereby the user has to verify his or her identity at the printer before the document is printed or released. To reduce the risk of personal data being extracted from the MFP's local storage device, some possible measures include:

- turning on the encryption feature to encrypt data in the storage device, where available;
- regularly purging print jobs that are no longer required from the storage device; and
- overwriting the storage device before disposal or returning the machine to the vendor.

Example 5

Organisation Y has an old photocopier and decides to replace it. Y sells the photocopier to a second hand shop without realising that there is a storage device built into the photocopier. Person X buys the old photocopier from the second hand shop and is able to retrieve copies of personal data of Y's customers that were captured by the photocopier's internal storage device.

Organisation Y should first check whether the MFP contains any storage device and to arrange for the data stored in such device to be securely deleted before disposal of the MFP.

Example 6

Organisation Y uses an MFP that is connected to the office computer network. The MFP's security features are activated. The default administrator password for the MFP is changed to a strong password. Data stored at the MFP is encrypted. Past print jobs are set to be purged immediately after the document is printed. Audit logging is turned on. An employee has been tasked to shred all uncollected printouts from the MFP at the end of every working day.

Table 10: Security for Printers, Copiers, Scanners and Fax Machines (MFPs)	
Good practices	
a	Identify and take stock of the MFPs within your organisation.
b	Put in place a process to check that any MFP scheduled for destruction, removal or sale does not contain any personal data in the internal storage device.
c	Remove (return to owner or destroy) any uncollected printouts and faxes that contain personal data.
Enhanced practices	
d	Use the secure print/pull print feature if provided by the MFP.
e	Use a fax cover sheet for documents being faxed, stating the recipient and sender details, the security classification and the number of pages in the document.
f	Provide advance notice to the fax recipient, such as by asking the recipient to wait at the fax machine before sending the fax.

13 Databases

13.1 Databases are used to store and manage data. Some could contain personal data, and organisations need to put in place adequate protection for these databases.

13.2 Different database products and their various editions tend to have different security features. Organisations should consider their security requirements when selecting a database product. Considerations should include identifying the types of personal data to be stored and the risk of damage to the individual should such data be compromised.

13.3 The types of personal data held should be reviewed and the need to store such personal data in encrypted form assessed. Typically, encryption may be performed for the entire

database or only for selected fields within the database. Alternatively, data may be encrypted before storing in the database.

13.4 In determining where to site databases, databases should be placed in the most secure network zone and segregated from the Internet, or even the organisation's internal computer network. Like other servers and parts of the computer network, security for databases should be regularly reviewed and improved upon.

13.5 Databases are often backed-up. These backups need to be similarly or even better protected than the database itself, in particular when the back-up is stored offsite.

Table 11: Database Security	
Good practices	
a	Strictly control users' direct access to the database, e.g. to execute arbitrary SQL commands or access the database schema.
b	Check that the database is hardened and not placed in a vulnerable spot within the network.
c	Encrypt confidential or sensitive personal data that has a higher risk of adversely affecting the individual should it be compromised. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.
Enhanced practices	
d	Encrypt personal data stored in database.
e	Log database activities, such as any changes to the database and data access activities to track unauthorised activities or anomalies.
f	Strictly control remote administrator access to the database.

14 Email

14.1 Email and other communication systems are typically used on a day-to-day basis amongst employees, as well as with external parties. These communications may contain personal data.

14.2 Encrypting emails or attachments, sending them through an encrypted channel, or sending the information via other secure means may reduce the risk of personal data being compromised in the event that an email containing personal data was sent to an unintended party or intercepted by cyber attackers.

14.3 Encryption may not be necessary for all emails. However, where emails contain confidential or sensitive personal data that has a higher risk of adversely affecting an individual if such personal data is compromised, organisations should then consider adopting encryption.

14.4 Where encryption of email is not supported, consider moving the personal data into an attached document which is protected. Protection can be provided by encryption[5] or by password protection[6] - methods often provided by commonly available application software.

Table 12: Email Security	
Good practices	
a	Install anti-malware software to the email server and clients. Keep the software updated and perform scans regularly.
b	Before sending out emails, review all recipients to ensure there is no unintended recipient.
c	Encrypt or password protect attachments containing personal data that has a higher risk of adversely affecting the individual should it be compromised. The password should be communicated separately. For encryption, review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure, whereas for password protection ensure a strong password is used.
Enhanced practices	
d	Make use of security features provided by some email systems to detect and prevent personal data from being sent out.

15 Websites and Web Applications

15.1 Websites and web applications are often used to communicate or provide services to customers or the public. A website is generally used to disseminate information whereas a web application tends to be more interactive and may allow a user to perform transactions such as buying items or checking personal account information.

15.2 Websites and web applications may be connected to a database at the backend. The database may contain personal data, such as information about an organisation's customers.

[5] The encryption key can be directly specified or derived from a password

[6] Whereby access to the file is protected using a password but the file itself is not encrypted

15.3 Precautions should be taken by organisations that have public-facing websites against common forms of malicious activities on websites and web applications, which include:

- Injection attacks – where data is input into a web application to facilitate the execution of malicious data in an unexpected manner. The most common type of injection attack is SQL injection. This sends malicious database instructions disguised as user input from a website or web application to a database. It potentially allows attackers to access, modify and delete data.

- Cross-site scripting ("**XSS**") - where attackers introduce malicious programs into web pages viewed by other users. XSS attacks can cause a website or web application to be deceived into activating malicious programs. It allows attackers to deface websites, redirect users to malicious websites, or hijack users' activities.

- Buffer overflow attacks – where malicious programs are used to send more data to a buffer, a temporary data storage area, than it was intended to hold. As buffers can contain only a limited amount of data, the extra information will overflow into adjacent buffers, corrupting or overwriting the data held in them.

15.4 Precautions include:

- performing careful validation of user input;
- using secure methods to make calls to application programming interfaces ("**API**"); and
- applying secure connection technologies or protocols, such as Transport Layer Security ("**TLS"**), to secure the link between a website or web application and a web browser.

15.5 Developers sometimes build 'backdoors' in the form of 'secret' URLs or debugging logs that allow access to data without user authentication. These data may include personal data. Usually this is only meant for testing purposes or temporarily periods, but the risk occurs when the backdoors are forgotten, thereby becoming a permanent feature. URLs to such functions can be discovered by attackers using automated means, even if the URLs are not published or are made known only to authorised users. Relying on the robots exclusion protocol (robots.txt) to hide webpages is also not recommended, as it is not mandatory for internet search engines to follow the directives.

Table 13: Websites and Web Application Security	
Good practices	
a	Perform data validation on user input to prevent buffer overflow attacks, injection attacks and XSS attacks.

b	Ensure that files containing personal data are not accidentally made available on a website or through a web application. Even if the link to such files is not published, it may still be discovered and accessed.
c	Perform cookie data validation, as well as URL validation to correspond with the session in use.
d	Do not allow 'backdoors' that allow bypass of user authentication to access personal data. Do not rely on the robots exclusion protocol (robots.txt) to hide webpages.
Enhanced practices	
e	Apply secure connection technologies or protocols, such as TLS, to websites and web applications that handle personal data.
f	Perform web application scanning and source code analysis to help detect web vulnerabilities. Vulnerabilities to look out for could include those in the Open Web Application Security Project (OWASP) "Top Ten" list or similar.
g	Configure web servers to disallow the browsing of file directories.
h	Do not store production data that contains personal data in non-production environments for testing or other purposes. Non-production environments include a network, operating system or other systems that are used as a development area or test bed for new software or technologies.
i	Disallow multiple sessions for the same user, where the use case clearly does not need support for multiple sessions.

16 Patching

16.1 Software may contain errors or bugs. Some of these lead to security vulnerabilities. Software developers generally release security patches over time to address the vulnerabilities.

16.2 Software that is not (or no longer) supported by its developer may be at greater risk as there is no party responsible for resolving security issues.

16.3 Vulnerabilities discovered are often published, hence cyber attackers are well aware of vulnerabilities available for exploiting.

16.4 It is therefore important for organisations to keep their software updated or patched regularly to minimise their vulnerabilities.

Table 14: Patching	
Good practices	
a	Test and apply updates and security patches as soon as they are available to relevant components of the organisation's ICT systems. These components include those described in this guide, i.e. network devices, servers, database products, operating systems and application software on computers and mobile devices, software libraries, programming frameworks, firmware (to control hardware).
Enhanced practices	
b	Ensure that software patches are downloaded from a legitimate source and preferably, digitally signed by the software vendor, to ensure the integrity of the software patch.

17 ICT Outsourcing and Software Products

17.1 It is common practice for organisations, especially SMEs, to outsource their ICT requirements to be fulfilled by vendors.

17.2 Note that both an organisation and its vendors are responsible for protecting the personal data handled by the organisation's ICT systems.

17.3 Software (whether provided as part of ICT vendors' solutions or self-implemented by the organisation) can be broadly classified into two types – bespoke or ready-made. Bespoke software is designed according to an organisation's specific needs. On the other hand, the design of ready-made software cannot be changed; typically, customisation is limited to configuration settings. Ready-made software includes "commercial off-the-shelf" software, social media platforms such as Facebook and Google+, and website or blog creation systems such as WordPress, Joomla and Tumblr. Some ready-made software allow add-on capabilities through plugins. In this context, open source software are also ready-made[7]. Ready-made software requires less time to deploy. However, organisations need to understand the capabilities, features and limitations of ready-made software. Failing which, organisations run the risk of not knowing how such systems collect, protect, use and disclose personal data.

17.4 For bespoke software, ICT vendors should be clearly informed by the organisation when personal data is to be handled, to allow the design of the system to take that into account and provide sufficient protection.

17.5 For ready-made software, organisations should give consideration as to whether sufficient protection is provided to personal data. If unfamiliar, organisations should

[7] Organisations may be able to modify source code made available for open source software, but in general it is quite common for open source software to be used in the original form or with minimal modifications.

find out how the software collects, protects, uses and discloses personal data before using it. This applies to the overall software and plugins as well. Organisations should obtain a clear understanding of:

- The intended purpose of the software;
- How the software functions;
- How the software collects and processes personal data;
- Whether the software discloses or transfers out personal data;
- How the software protects personal data;
- How to implement the software and integrate it with existing components (if necessary) of the organisation; and
- How to configure the software correctly.

17.6 Unless an ICT system is entirely developed from scratch and deployed under full control of the organisation, it likely makes use of ready-made components or services to some extent. While such ready-made components or services cannot be completely controlled by the Organisations, Organisations should always ensure sufficient protection for the parts for which they retain control. This is analogous to the scenario where an organisation leases office space. The organisation first chooses an appropriate office where robust building security is provided by the building management. However, the organisation is still responsible for the security of its own office unit. The organisation may install a lock at its office entrance, an alarm system, CCTV, a safe, etc.

17.7 Employees should also be provided with the appropriate training to ensure proper usage of the software used.

17.8 Refer to the PDPC's *Guide on Building Websites for SMEs* for more information on considerations for protecting electronic personal data in the context of website development and maintenance from a business perspective.

Example 7

An organisation started an account on a social media platform to better engage its customers. A customer posted a query about product warranty on the organisation's 'wall' on the social media platform. Unfamiliar with using social media, the organisation included personal data in its reply to the customer, unaware that the reply could be publicly viewed.

Example 8

A mobile application developer decided to include an advertisement engine (a software component) in its mobile application, as part of a commercial deal with the advertisement

company. However, the advertisement engine also collected personal data about the application users and sent it back to the advertisement company's servers. The application developer was not aware of this.

Table 15: ICT Outsourcing	
Good practices	
a	For bespoke solutions: (i) Ensure that vendors are aware that the organisation intends to use their services to handle personal data. (ii) Spell out the organisation's security requirements in the contract(s) between the organisation and its vendors.
b	For ready-made solutions: (i) Acquire a clear understanding of the solution. (ii) Select solutions that offer sufficient protection to personal data. (iii) Select solutions that match the organisation's requirements well. (iv) Understand the features and limitations of the solution (including plugins) processing personal data, before putting it into use. (v) Provide protection for the parts of the ICT system or personal data that are still under direct control.

18 Cloud Computing

18.1 Cloud computing is an on-demand service model for IT provisioning that is often based on virtualisation and distributed computing technologies.

18.2 There are various cloud service models, including software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Depending on the cloud service model, organisations accept to relinquish varying level of control over personal data. It is generally regarded that with SaaS, organisations have the least control. The degree of control increases with PaaS and further with IaaS.

18.3 There are also various cloud deployment models, such as private clouds, public clouds, community clouds and hybrid clouds Similar to the service models, the type and amount of control relinquished by the organisation vary. It is generally regarded that organisations have the least controls with public clouds. Higher levels of control may be achieved with community and hybrid clouds, while private clouds offer the most control.

18.4 The design and operations of cloud computing differ to some extent from non-cloud systems. Organisations that adopt cloud services for the management of personal data

need to be aware of the security and compliance challenges that are unique to cloud services.

18.5 Organisations should consider the recommendations in this Guide for controls they are able to manage directly. Where cloud service providers are unable to customise a service for the organisation, the organisation must decide if the security measures put in place by the cloud service providers provides reasonable security for the personal data. Many cloud service providers publish a list of security measures offered. This can be used to help organisations make a decision on whether the level of protection is sufficient for the personal data being stored in the cloud. Organisations may refer to existing standards such as the Multi-Tier Cloud Security (MTCS)[8] or ISO 27018[9] for additional guidance.

19 Additional Resources

19.1 In developing this Guide, best practices from personal data protection agencies in other countries were considered. These agencies include the UK Information Commissioner's Office[10], the US Federal Trade Commission[11], the Office of the Privacy Commissioner of Canada[12] and the Office of the Australian Information Commissioner[13]. Representatives of the following associations were also consulted with in the development of this Guide:

- Association of Information Security Professionals (AISP)
- Association of Small and Medium Enterprises (ASME)
- International Information Systems Security Certification Consortium, Inc. ((ISC)²), Singapore Chapter
- Information Technology Management Association (ITMA)
- Information Technology Standards Committee (ITSC)
- Singapore Business Federation (SBF)
- Singapore Computer Society (SCS)
- Singapore infocomm Technology Federation (SiTF)

[8] The Multi-Tier Cloud Security Standard for Singapore (MTCS SS) has a self-disclosure requirement for Cloud Service Providers (CSPs) covering areas such as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, as well as incident and problem management. Certified CSPs are able to spell out the levels of security that they can offer to their users. Organisations that utilise cloud computing services are able to use the MTCS SS to better understand and assess the cloud security they require.
[9] ISO/IEC 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
[10] Website at http://ico.org.uk/
[11] Website at https://www.ftc.gov/
[12] Website at https://www.priv.gc.ca
[13] Website at http://www.oaic.gov.au/

19.2 Reference may be made to the following for more information:

- https://sso.agc.gov.sg/Act/PDPA2012
    a. *Personal Data Protection Act 2012*

- https://www.pdpc.gov.sg/ag
    b. *Chapter 17 (Protection Obligation) of the Advisory Guidelines on Key Concepts in the PDPA*, published by PDPC
    c. *Section 3 (Anonymisation) of the Advisory Guidelines on the PDPA for Selected Topics*, published by PDPC

- https://www.pdpc.gov.sg/og
    a. *Managing Data Breaches*, published by PDPC
    b. *Guide to Disposal of Personal Data on Physical Medium,* published by PDPC
    c. *Guide on Building Websites for SMEs,* published by PDPC in partnership with Cyber Security Agency of Singapore (CSA)

END OF DOCUMENT

Annex A1: Consolidated Checklist of Good Practices

Clear accountability		
1	Provide clear direction for ICT security goals and policies for personal data protection within the organisation.	☐
2	Identify and empower the person(s) accountable for personal data protection within the organisation.	☐
Standards, policies and procedures		
3	Establish and enforce ICT security policies, standards and procedures.	☐
4	Review and update ICT security policies, standards and procedures periodically to ensure relevance.	☐
5	Establish end user policies to prevent misuse of ICT systems.	☐
Risk Management		
6	Institute a risk management framework to identify the security threats to the protection of personal data, assess the risks involved and determine the controls to remove or reduce them.	☐
7	Assess the effectiveness of the risk mitigation controls periodically.	☐
8	Assess the security risks involved in out-sourcing or engaging external parties for ICT services and mitigate them.	☐
Classification and tracking		
9	Classify and manage the personal data by considering the potential damage (e.g. reputational or financial) to the individuals involved should the data be compromised.	☐
10	Conduct periodic checks for personal data stored in ICT systems. For personal data that is not required in any form anymore, securely dispose the data (refer to section 8). If there is a need to retain the data but not in identifiable form, e.g. for performing data analytics, consider anonymising the data.	☐
11	Conduct physical asset inventory checks regularly to ensure all computers and other electronic devices (e.g. portable hard drive, printer, fax machine etc) used to store or process personal data are accounted for.	☐

Security Awareness		
12	Educate employees on ICT security threats and protection measures for personal data. This includes the organisation's ICT security policies, standards and procedures.	☐
13	Keep ICT security awareness training for employees updated and conduct such training regularly.	☐
Compliance, Testing and Audits		
14	Conduct regular ICT security audits, scans and tests to detect vulnerabilities and non-compliance with organisational standards.	☐
15	Apply prompt remedial actions to detect security vulnerabilities and any non-compliance with established policies and procedures.	☐
16	Implement measures to ensure ICT system logs are reviewed regularly for security violations and possible breaches.	☐
Authentication and Passwords		
17	Determine a suitable authentication method, single factor or multi-factor, for accessing personal data based on the risk of damage to the individual in case of a data breach.	☐
18	Determine a suitable maximum number of attempts allowed for a user to authenticate his or her identity based on the type of data to be accessed.	☐
19	Implement account lockout when the maximum number of attempts is reached, to prevent dictionary or brute-force attacks, which refer to methods of systematically checking all possible keys or passwords until the correct one is found.	☐
20	Password used for authentication has a length of at least 8 characters containing at least 1 alphabetical character and 1 numeric character.	☐
21	When password used for authentication is typed in, it is to be hidden under placeholder characters such as asterisks or dots.	☐
22	Password used for authentication is encrypted during transmission and also encrypted or hashed in storage. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.	☐
23	Users are required to change their passwords regularly. The frequency should be based on the risk of damage to the individual if the data is compromised.	☐

24	Change default passwords to strong passwords at the earliest possible opportunity.	☐
Authorisation		
25	Implement authorisation mechanisms and processes to check if the person accessing the system has appropriate access rights to data requested within the system.	☐
26	Define user roles or groups for systems that enable access to personal data. Access rights for each user role or group should be clearly defined and reviewed regularly.	☐
27	Grant a user only the necessary access rights to personal data within systems to fulfil their role or function.	☐
28	Track and review usage of accounts and their associated access rights regularly. Remove or change access rights for unused or obsolete accounts promptly.	☐
29	Log all successful and failed access to systems to help detect unauthorised attempts to gain access to them.	☐
Destruction of Data		
30	Identify storage media to be destroyed or sold, and put in place a process to track whether personal data had been stored on them.	☐
31	Perform secure deletion, erasure or destruction of electronic personal information on storage media before redeploying, exchanging or disposing of the media.	☐
32	Perform physical or other known methods of destruction of storage media such as degaussing and incinerating when secure deletion, erasure or deletion of personal data stored on the media is not possible. This may be the case with faulty storage media.	☐
Computer Network Security		
33	Equip networks with defence devices or software.	☐
34	Review configuration settings regularly to ensure they correspond to current requirements.	☐
35	Design and implement the internal network with multi-tier or network zones, segregating the internal network according to function, physical location, access type etc.	☐

Security of Personal Computers & Other Computing Devices		
36	Protect computers by using password functions.	☐
37	Install anti-malware software such as anti-virus, anti-spyware, and software-based firewall on computers. Keep them updated and perform scans regularly.	☐
38	Encrypt sensitive personal data, which has a higher risk of adversely affecting the individual should it be compromised. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.	☐
39	Prevent unauthorised personnel from viewing the screens of personal computers easily, such as by using privacy filters, or through positioning of the personal computer.	☐
40	Enforce password policy as indicated in Table 4.	☐
41	Implement additional controls for shared computers to prevent access to personal data, e.g. those keyed in by another user.	☐
Portable Computing & Removable Storage Media Security		
42	Identify and take stock of the portable computing devices and removable storage media used by your organisation.	☐
43	Minimise storage of personal data on portable computing devices and removable storage media. Remove personal data that is no longer required as soon as possible. (For additional information, refer to Section 8)	☐
44	Secure portable computing devices and removable storage media when not in use. This can be done by keeping them under lock and key, attaching them to a fixture by a security cable, hand-carrying, and not leaving them unattended.	☐
45	Configure portable computing devices to automatically lock upon a period of inactivity, whereby a password is required to resume usage.	☐
46	Assess the applications that users can install and establish a policy for the use and tracking of the organisation's portable computing devices and removable storage media.	☐
Security for Printers, Copiers, Scanners and Fax Machines (MFPs)		
47	Identify and take stock of the MFPs within your organisation.	☐
48	Put in place a process to check that any MFP scheduled for destruction, removal or sale does not contain any personal data in the internal storage device.	☐

49	Remove (return to owner or destroy) any uncollected printouts and faxes that contain personal data.	☐
Database Security		
50	Strictly control users' direct access to the database, e.g. to execute arbitrary SQL commands or access the database schema.	☐
51	Check that the database is hardened and not placed in a vulnerable spot within the network.	☐
52	Encrypt confidential or sensitive personal data that has a higher risk of adversely affecting the individual should it be compromised. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.	☐
Email Security		
53	Install anti-malware software to the email server and clients. Keep the software updated and perform scans regularly.	☐
54	Before sending out emails, review all recipients to ensure there is no unintended recipient.	☐
55	Encrypt or password protect attachments containing personal data that has a higher risk of adversely affecting the individual should it be compromised. The password should be communicated separately. For encryption, review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure, whereas for password protection ensure a strong password is used.	☐
Websites and Web Application Security		
56	Perform data validation on user input to prevent buffer overflow attacks, injection attacks and XSS attacks.	☐
57	Ensure that files containing personal data are not accidentally made available on a website or through a web application. Even if the link to such files is not published, it may still be discovered and accessed.	☐
58	Perform cookie data validation, as well as URL validation to correspond with the session in use.	☐
59	Do not allow 'backdoors' that allow bypass of user authentication to access personal data. Do not rely on robots exclusion protocol (robots.txt) to hide webpages.	☐

Patching		
60	Test and apply updates and security patches as soon as they are available to relevant components of the organisation's ICT systems. These components include those described in this guide, i.e. network devices, servers, database products, operating systems and application software on computers and mobile devices, software libraries, programming frameworks, firmware (to control hardware).	☐
ICT Outsourcing		
61	For bespoke solutions: i. Ensure that vendors are aware that the organisation intends to use their services to handle personal data. ii. Spell out the organisation's security requirements in the contract(s) between the organisation and its vendors.	☐
62	For ready-made solutions: i. Acquire a clear understanding of the solution. ii. Select solutions that offer sufficient protection to personal data. iii. Select solutions that match the organisation's requirements well. iv. Understand the features and limitations of the solution (including plugins) processing personal data, before putting it into use. v. Provide protection for the parts of the ICT system or personal data that are still under direct control.	☐

Annex A2: Consolidated Checklist of Enhanced Practices

Authentication		
1	Assign unique and distinct user ID to individual users.	☐
2	Encourage users not to use passwords that can be easily deduced, such as their birth date or name.	☐
3	Users to change system-generated password upon first login.	☐
4	Discourage users from using the same password across different systems or applications.	☐
5	The same password is not allowed to be reused within the last 3 changes.	☐
6	Password used comprises both lowercase and uppercase characters.	☐
7	Password used comprises special characters such as '!', '&',etc.	☐
Computer Network Security		
8	Apply secure connection technologies or protocols when transmitting electronic personal data, such as over a computer network or from one network to another.	☐
9	Disable unused network ports.	☐
10	Monitor LAN/WiFi regularly and remove unauthorised clients and WiFi access points.	☐
11	Use two-factor authentication and strong encryption for remote access. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.	☐
12	Use network proxies to restrict employee access to known malicious websites.	☐
13	Disallow remote network administration.	☐
Security of Personal Computers & Other Computing Devices		
14	Disallow anonymous or guest logins.	☐
15	Disallow non-administrator users from booting up a computer using external or removable storage media.	☐
16	Disallow non-administrator employees from installing software or changing security settings, except on a need-to basis. Keep administrator accounts for administrator use only.	☐
17	Remove unused software and turn off unnecessary services from computers.	☐

18	Install or activate Application Control solutions.	☐
Portable Computing & Removable Storage Media Security		
19	Install and activate remote device locking and wiping features, which allow the portable computing devices to be locked and local data erased from any location in the event of theft or loss of device.	☐
20	Turn off wireless communication features such as Wi-Fi and Bluetooth when these are not in use.	☐
21	Connect to external WiFi access points carefully and secure communications, e.g. by using Virtual Private Networks (VPN).	☐
Security for Printers, Copiers, Scanners and Fax Machines (MFPs)		
22	Use the secure print/pull print feature if provided by the MFP.	☐
23	Use a fax cover sheet for documents being faxed, stating the recipient and sender details, the security classification and the number of pages in the document.	☐
24	Provide advance notice to the fax recipient, such as by asking the recipient to wait at the fax machine before sending the fax.	☐
Database Security		
25	Encrypt personal data stored in database.	☐
26	Log database activities, such as any changes to the database and data access activities to track unauthorised activities or anomalies.	☐
27	Strictly control remote administrator access to the database.	☐
Email Security		
28	Make use of security features provided by some email systems to detect and prevent personal data from being sent out.	☐
Websites and Web Application Security		
29	Apply secure connection technologies or protocols, such as TLS, to websites and web applications that handle personal data.	☐
30	Perform web application scanning and source code analysis to help detect web vulnerabilities. Vulnerabilities to look out for could include those in the Open Web Application Security Project (OWASP) “Top Ten” list or similar.	☐
31	Configure web servers to disallow the browsing of file directories.	☐

32	Do not store production data that contains personal data in non-production environments for testing or other purposes. Non-production environments include a network, operating system or other systems that are used as a development area or test bed for new software or technologies.	☐
33	Disallow multiple sessions for the same user, where the use case clearly does not need support for multiple sessions.	☐
Patching		
34	Ensure that software patches are downloaded from a legitimate source and preferably, digitally signed by the software vendor, to ensure the integrity of the software patch.	☐

BROUGHT TO YOU BY

IN PARTNERSHIP WITH