PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Is Personal Data Safe With Your Organisation?

Electronic Personal Data Protection for Organisations

Protecting the personal data of customers, employees and other individuals is increasingly important in today's digital world, where more and more information is being stored in electronic devices and IT systems, which can be easily lost, stolen or misused.

The Personal Data Protection Act (PDPA) was hence established to ensure that organisations take care of personal data under their possession or in their control. Breaching the PDPA could damage the reputation of your business, especially if the breach is publicised, causes financial loss or harm to affected individuals.

HOW CAN ELECTRONIC DATA BE COMPROMISED?

There are several ways that electronic personal data can be compromised. These include malicious activities, storage devices that are inadequately protected and simple human error.

Here are some examples:

Malicious Activities

- Hacking or other unauthorised access of databases
- Physical attacks (e.g. use of skimming devices on Automated Teller Machines, or ATMs)
- Social engineering (e.g. phishing scams and the circulation of malware-laden email attachments)
- Unauthorised access or misuse of personal data by employees or vendors

Human Error

- Loss of electronic devices or portable storage devices containing personal data
- Not disposing of electronic data properly
- Emailing personal data to the wrong recipient

System/Device Error

- Fault or weakness in a system's or device's program code causing it to reveal personal data to incorrect parties (e.g. a bug in an online portal allowing someone to access another person's data)

WHAT ARE SOME GOOD INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) PRACTICES TO IMPLEMENT?

Here are some recommendations to help your organisation protect electronic personal data.

1. Managing Access Controls

Your organisation can reduce human error by allowing only the authorised person(s) to access personal data, and ensure that only known users and sources do so because they need to.

Protect personal data through user accounts and passwords:

- Provide each user with a unique username and password, and prompt them to change their passwords regularly.
- Limit the number of failed login attempts and lock the user out of the account when the limit has been reached.
- Hide the password when the user is keying it in (to reduce the chances of it being viewed by others).
- Cancel a user's access promptly when he leaves the organisation or is away for a long period.

TIP

A strong password has a minimum of eight characters with at least one alphabetical character, one numeric character, one special character and a mix of capital and small letters.

2. Securing Electronic Devices Used by Employees

Hackers often take advantage of weaknesses in computer systems or software to access personal data. Limit this by regularly checking for patches to any software or hardware involved in personal data, and applying them as soon as they are available.

TIP

Vendors usually issue alerts on patches, so check with them.

Here are some other ways to secure your organisation's devices:

Personal Computers

- Turn on the password features.
- Install software such as anti-virus, anti-spyware and personal firewall. Keep these software updated and perform scans regularly.

Portable Devices
(e.g. Laptops, Tablets, Memory Cards, Thumbdrives, Hard Disks)

- Secure such devices and storage media when not in use by keeping them under lock and key, hand-carrying them and not leaving them unattended.
- Use strong passwords or encryption to protect the data.

Printers, Copiers, Fax Machines

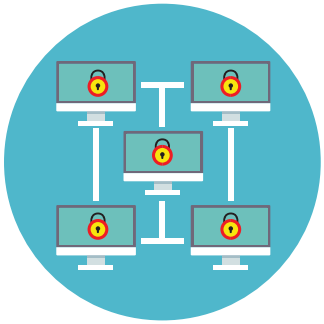
- Ensure that any machine to be destroyed, removed or sold does not contain any personal data (see page 5 for more information).
- Destroy any uncollected printouts and faxes that contain personal data as soon as possible.

3. Protecting Databases

Some measures that can help in the protection of personal data in databases include:

- preventing users from accessing the database without proper clearance; and
- encrypting confidential or sensitive personal data.

4. Securing Computer Networks



Internal computer networks are often connected to external networks, such as the Internet. Any weakness in these systems increases the risk of cyber theft. Your organisation can increase security of its networks by:

- equipping them with security devices or software such as firewalls or anti-malware applications;
- regularly checking that the settings are appropriate for the current requirements; and
- separating and limiting access between the different parts of the network. For example, the web server should be separate from the internal file server, so that if the web server is compromised, the hacker will not have access to personal data kept in the internal file server.

5. Protecting Websites and Web Applications

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

Check that:

- measures have been taken to secure websites and applications against Structured Query Language (SQL) injection and cross-site scripting attacks; and
- no unnecessary files containing personal data is made available online.

6. Safeguarding Email Content

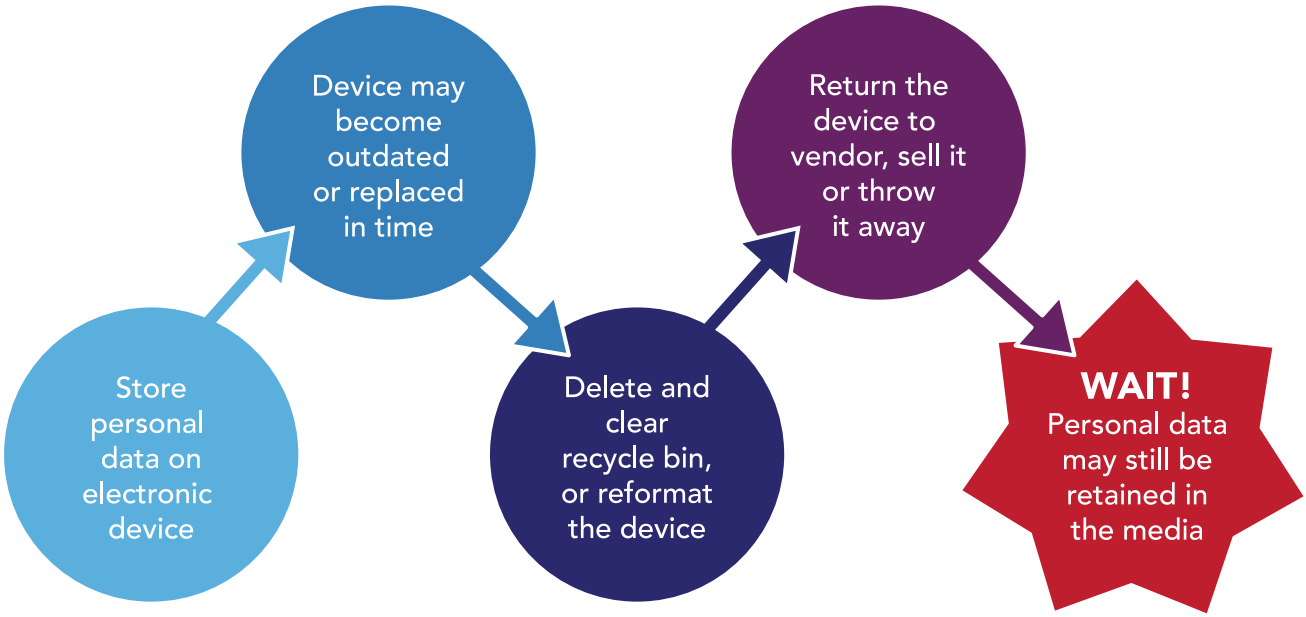
Email and other communications systems often contain personal data and can be protected with anti-malware or other email security software.

Your organisation can also encrypt the contents of emails to reduce the risk of personal data being compromised in case they are sent to the wrong person.

TIP
Encryption can be applied on a case-by-case basis.

HOW CAN MY ORGANISATION SAFELY DISPOSE OF ELECTRONIC PERSONAL DATA?

Make it a point to regularly review all personal data and remove any that is no longer needed. It is a common assumption that deleting the files and clearing the recycle bin destroys them completely. However, the computer simply hides them from view and there are certain software that can recover such "deleted" files.



By taking the following additional steps, your organisation can permanently destroy or remove electronic data:

- Use specific software that can overwrite selected files or the entire storage drive.
- Use specialised hardware appliances (e.g. a degausser machine which produces a strong electromagnetic field that can destroy magnetically recorded data).
- Physically destroy the storage device by crushing, drilling or shredding it.

TIP

For outsourced IT services, put in frameworks to make sure the vendors treat personal data with the same level of security as your organisation does.

HOW ELSE CAN MY ORGANISATION PROTECT PERSONAL DATA?

Your organisation can further improve data protection through good planning and governance of ICT.

Follow the steps below to identify possible risks and improve data protection.

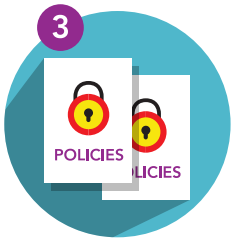
Step 1 - Appoint a Data Protection Officer

Place one person (or more) in charge of ensuring your organisation is compliant with the PDPA. He or she should:

- put in place policies for handling personal data in electronic or non-electronic forms;
- ensure these policies are communicated to customers; and
- handle any queries or complaints about personal data.

Step 2 - Review the Personal Data Inventory

Understand precisely how, when and where personal data is collected and stored. Know the purpose for collecting the data and get consent to use it.



Step 3 - Enforce ICT Security Policies, Standards and Procedures

Implement policies, standards and procedures that protect personal data. Review them regularly to ensure they include changes in business practices or technological advancements.

Step 4 - Communicate Internally

Communicate your organisation's data protection policies to all employees and contract staff, as well as sub-contractors who handle personal data. Everyone needs to know how they can help protect personal data and be aware of the internal processes concerning data protection.

Step 5 - Establish an Internal Audit Policy

Conduct regular internal audits to ensure your organisation's processes are in line with the PDPA.

WHERE CAN I GET MORE INFORMATION?

For more information, please refer to the associated Guide to Securing Personal Data in Electronic Medium for IT professionals at the Personal Data Protection Commission's website www.pdpc.gov.sg or visit www.gosafeonline.sg/smes by the Cyber Security Awareness Alliance (Singapore).

BROUGHT TO YOU BY

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

IN PARTNERSHIP WITH

CSA SINGAPORE