

CARE OF PERSONAL DATA PROTECTION

Assure your customers and earn their trust by adopting good data protection practices today!

PROTECTION OBLIGATION



Put in place reasonable security arrangements to protect personal data from unauthorised access, collection, use, disclosure or similar risks.



Classify the personal data to better manage housekeeping.



Regularly review the protection policies and processes for the personal data in your possession or control.

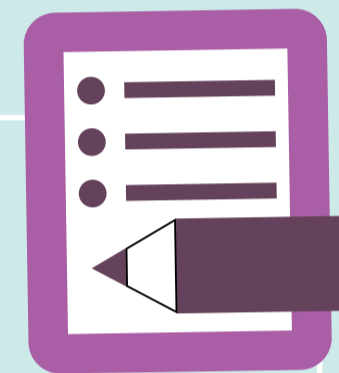


Implement appropriate levels of security for personal data of varying levels of sensitivity.

EXAMPLES OF DATA SECURITY MEASURES

i) Administrative Measures

- Require employees to be bound by confidentiality obligations in their employment agreements.
- Implement robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations.
- Conduct regular training sessions to impart good practices in handling and protecting personal data.
- Ensure that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.



ii) Physical Measures

- Mark confidential documents clearly and prominently.
- Store confidential documents in locked file cabinet systems.
- Restrict employee access to confidential documents on a need-to-know basis.
- Use privacy filters to minimise unauthorised personnel from viewing personal data on laptops.
- Proper disposal of confidential documents that are no longer needed, through shredding or similar means.

iii) Technical Measures

- Ensure computer networks are secure.
- Adopt appropriate access controls such as stronger authentication measures where appropriate.
- Encrypt personal data to prevent unauthorised access.
- Activate self-locking mechanisms for the computer screen if the computer is left unattended for a certain period.
- Install appropriate computer security software and use suitable computer security settings.
- Dispose of personal data in IT devices that are to be recycled, sold or disposed.
- Use the right level of email security settings when sending and/or receiving highly confidential emails.
- Update computer security and IT equipment regularly.
- Ensure that IT service providers are able to provide the requisite standard of IT security.



CLICK
HERE



SUPPLEMENTARY RESOURCES

1. Guide to managing data breaches.
2. Guide to securing personal data in electronic medium.



The more trusted a brand is, the more willing customers are to share their personal data.



For more information, refer to the PDPC's Advisory Guidelines on Key Concepts in the PDPA at www.pdpc.gov.sg