Compliance to PDPA: a quick guide
Introduction to data protection

The PDP Principles

Conclusion
1. DATA PROTECTION IN BRIEF


**Data Protection**

**What?**

- Data protection is all about securing data from unauthorized access, misuse and loss.

**Why it matters?**

- If personal data is stolen, privacy is not guaranteed which opens the windows to risk for identity and other security breaches.

**How?**

- Personal data governance
DATA PROTECTION

PERSONAL DATA PROTECTION ACT 2010

- Federal and State Governments
- Commercial transactions
- Non-commercial transactions
2. KEY TERMS
<table>
<thead>
<tr>
<th><strong>Personal Data</strong></th>
<th><strong>Processing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Any information which may identify a data subject, in which it may be identifiable by one type of personal data or/and a combination of other personal data.</td>
<td>Carrying out any operation or set of operations on personal data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Sensitive Personal Data</strong></th>
<th><strong>Commercial Transactions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Information relating to the physical or mental health or condition, political opinions, religious belief or other beliefs of a similar nature.</td>
<td>Any transaction of a commercial nature, which includes the exchange of goods or services, investments, agency, financing, banking and insurance.</td>
</tr>
</tbody>
</table>
Third Party

1) A relevant person in relation to a data subject, 
2) A data processor; or 
3) A person authorized in writing by the data user to process the personal data under the direct control of the data user.

Vital Interest

Matters relating to life, death or security of a data subject.
Any transaction of a commercial nature,

- whether **contractual or not** but does not include credit reporting business under the Credit Reporting Agency Act 2010
PERSONAL DATA

- Full Name
- D.O.B
- P.O.B

- IC
- Passport
- Driving License

- Residential address
- Phone Numbers
- Email
- IP address
- Geo-location

- Health/Genetic info.
- Health conditions

- Images

- Financial info.

- Religious belief
- Sexual orientation
- Political opinions
## Processing of Personal Data

<table>
<thead>
<tr>
<th>Control</th>
<th>Disclose</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collecting</td>
<td>Transfer</td>
<td>Correction</td>
</tr>
<tr>
<td>Holding</td>
<td>Transmission</td>
<td>Retrieval</td>
</tr>
<tr>
<td>Use</td>
<td>Dissemination</td>
<td>Erasure</td>
</tr>
<tr>
<td>Recording</td>
<td></td>
<td>Destruction</td>
</tr>
<tr>
<td>Storing</td>
<td></td>
<td>Modification</td>
</tr>
</tbody>
</table>

- **Control**: Collecting, Holding, Use, Recording, Storing
- **Disclose**: Transfer, Transmission, Dissemination
- **Access**: Correction, Retrieval, Erasure, Destruction, Modification
### Key Players

<table>
<thead>
<tr>
<th>Data User</th>
<th>Data Processor</th>
<th>Data Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>a person who either alone or jointly processes any personal data or has control over or authorizes the processing of any personal data.</td>
<td>any person, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.</td>
<td>an individual who is the subject of the personal data. e.g. students, patients, employees, citizens, non-citizens.</td>
</tr>
</tbody>
</table>
3. THE PRINCIPLES OF PDP
THE PRINCIPLES

1. General
2. Notice & Choice
3. Disclosure
4. Security
5. Retention
6. Data Integrity
7. Access
1- GENERAL

Processing

- Collect
- Use
- Disclose

**Lawful Purposes: Section 6 (2)**

- Consent Matters
  - Process personal data with consent

- Lawful Purposes
  - The processing is necessary and directly related to business activity

- Adequate
  - Not excessive and reasonable

- Record and maintain consent
  - Burden of proof

- Incapable Data Subject
  - Consent by an authorized person/body

- Age of consent
  - Consent for “minor” must be obtained from legal guardian
<table>
<thead>
<tr>
<th>Implicit</th>
<th>Valid</th>
<th>Explicit</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Implied</td>
<td>❑ Informed</td>
<td>❑ Expressed</td>
</tr>
<tr>
<td>❑ Voluntary</td>
<td>❑ Reasonable</td>
<td>❑ Verbal/non-verbal</td>
</tr>
<tr>
<td>❑ Deemed</td>
<td>❑ Voluntary</td>
<td>❑ Clear affirmative action</td>
</tr>
<tr>
<td>❑ Inferred by one’s action</td>
<td>❑ Specific</td>
<td>❑ Option to agree or disagree</td>
</tr>
<tr>
<td>❑ Pre-ticked boxes (by default)</td>
<td>❑ Current</td>
<td>❑ Active Opt-in</td>
</tr>
<tr>
<td>❑ Inferred by one’s action</td>
<td>❑ Capacity to consent</td>
<td>❑ Able to withdraw</td>
</tr>
<tr>
<td>❑ Pre-ticked boxes (by default)</td>
<td>❑ Unbundled</td>
<td></td>
</tr>
</tbody>
</table>

*difficult to prove in legal context but can be done under certain circumstances*
Managing consent
**Obtain**

**How to obtain?**
- Signing a consent clause on a paper form
- Ticking an opt-in box (paper)
- Click an opt-in button or link
- Inform clients that consent can be withdrawn
- Seek parental consent for under-aged children
- Do not bundle up consent with other matters by default

**Record**

**Who consented the processing?**
- Name, ID, Relation with Data Subject
- Keep a copy of the signed document

**When and how they consented?**
- Keep a copy of a dated document, online log, call log;
- Provide a form or phone no. or email for withdrawing consent;
- Keep a copy of the withdrawn consent (paper/digital)

**Manage**

**Check that the processing and the purposes have not changed**
- Keep a copy of the current version of the consent

**Keep all documents containing consents in a proper manner**
- All files/documents containing consents must be retrievable
By submitting the application for coverage, you consent to the collection of your personal information (whether through the phone or otherwise obtained) and such information may be held, used and disclosed to individuals, service providers and organizations associated with AIG Malaysia or any other selected third parties (within or outside of Malaysia, including reinsurance and claims investigation companies and industry associations) for the purpose of storing and processing this insurance and providing subsequent service(s) for this purpose, AIG Malaysia's financial products and services, data matching, surveys, and to communicate with you for such purposes.

Consent

Clearly inform on the disclosure of information

Be transparent on the purpose of data collection
### 2- NOTICE AND CHOICE (Sec.7)

<table>
<thead>
<tr>
<th><strong>INFORMATION</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Collection</td>
<td>Purpose of data collection and further processed</td>
</tr>
<tr>
<td>The Processing</td>
<td>Whether personal data is processed by / on behalf of the Data user</td>
</tr>
<tr>
<td>The Source</td>
<td>The source where information on data subject is obtained</td>
</tr>
<tr>
<td>The Rights</td>
<td>Access and correction of personal data</td>
</tr>
<tr>
<td>The Disclosure</td>
<td>Disclosure of personal data to / by third parties</td>
</tr>
<tr>
<td>The Choices</td>
<td>Options and ways offered to limit processing</td>
</tr>
<tr>
<td>The Supply</td>
<td>Whether it is mandatory or voluntary to provide personal data</td>
</tr>
<tr>
<td>The Obligation and consequences</td>
<td>If it is obligatory to provide such personal data, inform the consequences if not provided</td>
</tr>
</tbody>
</table>

©Personal Data Protection Commissioner
Serving the notice

WHO?
New and existing:
- Clients
- Employees

WHY?
- Assurance
- Legal obligation
- To inform the purposes of data collection
- Provides contact info for inquiries/complaints

WHEN?
- Obtaining consent
- Providing services

HOW?
- Clear and straightforward language
- Appealing and intelligible
- Online/offline
<table>
<thead>
<tr>
<th></th>
<th>FRAMEWORK OF A NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Brief information on company and its practice in data protection</td>
</tr>
<tr>
<td>2</td>
<td>Collection and processing of personal data</td>
</tr>
<tr>
<td>3</td>
<td>Description of the personal data collected by data user</td>
</tr>
<tr>
<td>4</td>
<td>Purposes of collection</td>
</tr>
<tr>
<td>5</td>
<td>Sources of personal data</td>
</tr>
<tr>
<td>6</td>
<td>Disclosure to third parties/subsidiaries/authority bodies</td>
</tr>
<tr>
<td>7</td>
<td>Transfer of personal data overseas</td>
</tr>
<tr>
<td>8</td>
<td>Security measures to protect personal data</td>
</tr>
<tr>
<td>9</td>
<td>Retention of personal data</td>
</tr>
<tr>
<td>10</td>
<td>Access and correction of personal data</td>
</tr>
<tr>
<td>11</td>
<td>Consequences of failing to supply PD;</td>
</tr>
<tr>
<td>12</td>
<td>Marketing and promotional activities</td>
</tr>
<tr>
<td>13</td>
<td>Data subject’s obligations</td>
</tr>
<tr>
<td>14</td>
<td>For Inquiries (contact person)</td>
</tr>
</tbody>
</table>

©Personal Data Protection Commissioner
RM0: In case you missed it, in a continuous effort to improve our services, we have also updated our privacy policy. Visit https://www.celcom.com.my/legal/privacy-notice for details. Sincerely, Celcom.
3- DISCLOSURE (Sec. 8)

1. Data Subject
2. Data User
3. Third Parties

Process -> Disclosure
*Consent

©Personal Data Protection Commissioner
DISCLOSURE LIST:

For the purpose of Section 8 (b) –

Data user shall keep and maintain a list of disclosures of personal data that have been or are being processed by a third party.

<table>
<thead>
<tr>
<th>NO.</th>
<th>THIRD PARTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Close family member of Data Subject (Parents, Spouse, Siblings)</td>
</tr>
<tr>
<td>2.</td>
<td>Any person notified and authorized by the Data Subject</td>
</tr>
<tr>
<td>3.</td>
<td>Federal Government or State Government requesting information from the Data User</td>
</tr>
<tr>
<td>4.</td>
<td>Financial institutions</td>
</tr>
<tr>
<td>5.</td>
<td>Agents/Contractors/Consultants/Vendors/External Auditors/Counsellors/Data Processor Appointed by the Data User</td>
</tr>
<tr>
<td>6.</td>
<td>Approved bodies where employees contributions are remitted:</td>
</tr>
<tr>
<td></td>
<td>- Social Security Organisation (SOCSO)</td>
</tr>
<tr>
<td></td>
<td>- Pusat Zakat</td>
</tr>
<tr>
<td></td>
<td>- Baitulmal</td>
</tr>
<tr>
<td></td>
<td>- Lembaga Tabung Haji</td>
</tr>
<tr>
<td></td>
<td>- Koperasi</td>
</tr>
<tr>
<td></td>
<td>- Employees Provident Fund (EPF)</td>
</tr>
<tr>
<td>7.</td>
<td>Any person/party appointed by the Data User to recover the outstanding debt of the Data User</td>
</tr>
<tr>
<td>8.</td>
<td>Merchants, VISA International Services Association, MasterCard International Incorporated and other card associations (in relation to credit cards issued to Data Subject) for the purpose of payment of electricity bill or other services of the Data User</td>
</tr>
<tr>
<td>9.</td>
<td>The parties that the Data User may transfer rights and obligations pursuant to the agreement endorsed with the Data Subject</td>
</tr>
<tr>
<td>10.</td>
<td>Panel doctors/clinics/hospitals pharmacist appointed by the Data User</td>
</tr>
<tr>
<td>11.</td>
<td>Panel lawyers/legal advisors appointed by the Data User</td>
</tr>
<tr>
<td>12.</td>
<td>Wholly owned subsidiaries of the Data User</td>
</tr>
</tbody>
</table>
Permitted disclosure under the law (Sec. 39)

- Crime Prevention/Detection
- Public interest
- Law / Court orders
- Tax
- Regulatory functions
- Statistics/Research
- Journalistic

©Personal Data Protection Commissioner
Reasonable and practical measures to protect data from:

- Loss
- Misuse
- Modification
- Destruction
- Accidental access/disclosure

**No exemption for Security Principle**
Reasonable Steps

01 WHAT
- Paper
- Electronic

02 WHERE
- Secured environment
- Level of security

03 WHEN
- Sharing
- Portability
- Transfer
- Access

04 HOW
- Technical
- Policy/SOP
- Training

05 WHO
- Top Mgmt.
- Middle Mgmt.
- Personnel
<table>
<thead>
<tr>
<th><strong>Do's</strong></th>
<th><strong>Don'ts</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Controls:</strong></td>
<td>× Exposure:</td>
</tr>
<tr>
<td>- Keep paper files locked in cabinets</td>
<td>- Viewing or discussing personal information in public/online</td>
</tr>
<tr>
<td>- Activate a security system at high-risk location for theft or unauthorized access.</td>
<td>- Access to all personnel</td>
</tr>
<tr>
<td>- Limit access to computer systems or databases</td>
<td>× Poor physical and ICT/cyber security practice:</td>
</tr>
<tr>
<td>- Restrict access to sensitive documents</td>
<td>- Sharing log-in credentials with others</td>
</tr>
<tr>
<td><strong>Enhance data security:</strong></td>
<td>- Poor Password Management</td>
</tr>
<tr>
<td>- Use reputable cloud computing services</td>
<td>- Poor Disaster Recovery/Backup solution</td>
</tr>
<tr>
<td>- Establish an incident management plan</td>
<td>- Use unreliable cloud provider</td>
</tr>
<tr>
<td>- Improve network security</td>
<td>- Devices left unattended/ unprotected</td>
</tr>
<tr>
<td>- Control the use of removable media devices</td>
<td></td>
</tr>
<tr>
<td>- Encrypt data</td>
<td></td>
</tr>
<tr>
<td>- Keeping devices secure</td>
<td></td>
</tr>
<tr>
<td>- Keep passwords private</td>
<td></td>
</tr>
</tbody>
</table>

©Personal Data Protection Commissioner
5- RETENTION (Sec.10)

1. WHAT?
   Determine:
   - Period of data retention
   - Nature of data (active, inactive, archival, electronic)
   - What records does your business need to keep? (Legal / regulatory requirement)

2. WHO?
   Responsibilities:
   - Every personnel
   - Every business unit

3. WHEN?
   Personal data should be deleted at the end of retention period
   - Retention period should be reviewed if there is a need to keep them longer

4. HOW?
   Establish:
   - Retention policy
   - Disposal schedule and Checklist

   Destruction:
   - Irreversible
   - Secure
   - Documented
Disposal of records

01 Reasons for destruction
- To save time and cost of storage,
- To shift focus on the priority of the records
- To records from unauthorized access or loss
- To ensure accountability
- To meet legal requirements

02 Authorization
Seek approval prior to the disposal of records

03 Destruction methods
- For paper: shredding, pulping and burning sensitive documents
- Electronic/Digital: cutting, crushing, shredding reformatting

04 Documentation
- Keep a record of the documents which have been destroyed;
  - the description of documents
  - the disposal action taken
  - who authorized the disposal
  - who performed the disposal

05 Checklist
- The records have been approved for disposal
- Legal requirement/ administrative/ business purpose have been met
- The manner of destruction has been documented
- The means of destruction is appropriate
# RETENTION AND DISPOSAL OF RECORDS

## Retention And Disposal Schedule

<table>
<thead>
<tr>
<th>No.</th>
<th>Types of Records</th>
<th>Descriptions</th>
<th>Retention Period</th>
<th>Legal/ Administrative Requirements</th>
<th>Disposal Action (Hardcopy and Softcopy files/Attachments)</th>
<th>Disposal Authority</th>
</tr>
</thead>
</table>
| 1.  | Employee Files   | -Employee Personal File  
- Potential candidate  
- Training records | 7 years | -Limitation Act  
- HR policy | Delete after 7 years | General Mgr  
Assistant Mgr |
| 2.  | Financial Record  
- payroll  
- tax | -Employee pay histories  
- Salary ledger card/records  
- Copy of payroll sheets | 9 Years | -Income Tax Act | Delete after 9 years | General Mgr  
Assistant Mgr  
Accountant |
| 3.  | Attendance record | Staff and student | 5 years | HR policy | | |
| 4.  | Enquiry form | | 2 years | Customer service policy | | |
Outsourcing disposal activity

✓ Hire a reliable service provider which has
  ▪ comprehensive security;
  ▪ prioritizes safety, confidentiality and
    the environment.

✓ Ensure that destruction service is not
  limited to paper documents.

✓ All personal data in (electronic and non-
  electronic) must be disposed in a proper
  manner.

✓ Obtain certificate of destruction.
6- DATA INTEGRITY (Sec.11)

⭐ Personal data in your possession must be accurate, complete, up-to-date and not misleading

⚠ Ensure that the information you want to update is authentic, accurate and correct

⚙ Avoid data tampering

Truthful
Accurate
Complete
Verifiable
Retrievable

©Personal Data Protection Commissioner
The right for data subject to access and correct his personal data

WHEN?
- Data access requests must be complied not later than 21 days

HOW?
- Provide forms for data subject (physical/online)
- Any request in writing is considered as a valid request, regardless of the format.
PERSONAL DATA ACCESS REQUEST FORM

SECTION 1: TO BE FILLED IN BY DATA SUBJECT

Full Name (as per NRIC):

NRIC: (attach copy)

Contact Number:

Email address:

I, hereby certify that the information given in this form and any documents submitted are true and accurate.

Signature: ___________________________ Date: ___________________________

SECTION 2: TO BE FILLED BY RELEVANT PERSON (if the request is made on behalf of data subject)

A: Particular of Data Subject

Full Name (as per NRIC):

NRIC: (attach copy)

B: Particular of Relevant Person

Full Name (as per NRIC):

NRIC: (attach copy)

Contact Number:

Email address:

Relationship with data subject:

I, hereby certify that the information given in this form and any documents submitted are true and accurate.

I, hereby agreed that you may contact the Data Subject to verify my identity.

Signature: ___________________________ Date: ___________________________

SECTION 3: ACCESS OF PERSONAL DATA

Please provide a description of the personal data to be accessed

CHARGES

Do you need a copy of personal data? (tick ✓ in the relevant box) YES ☐ NO ✓

<table>
<thead>
<tr>
<th>Access without copy</th>
<th>Access with copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>General personal data</td>
<td>RM 2</td>
</tr>
<tr>
<td>Sensitive personal data</td>
<td>RM 5</td>
</tr>
</tbody>
</table>

©Personal Data Protection Commissioner
Common Security Breaches

01. Improper disposal of data
02. Unsecured data transfer
03. Overshare via Social Media
04. Accidental disclosure
Common refusal for compliance

“My business is too small”

“I have no idea where to start”

“Data security is too expensive”

“If you think compliance is expensive, try non-compliance.”

Paul McNulty
Former US Deputy Attorney General
4. THE DO’S AND DON’TS
MOST BREACHED PRINCIPLES

- Security
- Retention
- General
- Disclosure
General Principle

**Don’ts**

- Collect personal data excessively.
- Purposes of data collection is not clearly stated.
- Consent not recorded and maintained.
- Consent taken from person below 18.
- Pre-ticked consent by default (online).
<table>
<thead>
<tr>
<th>Name:</th>
<th><em>Male/Female</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. Telephone:</td>
<td><em>Number</em></td>
</tr>
<tr>
<td>Address:</td>
<td><em>Address</em></td>
</tr>
</tbody>
</table>

**HURDANGAN KECELAMASAN (ADAK - BERADIK) 2**

<table>
<thead>
<tr>
<th>Name:</th>
<th><em>Male/Female</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. Telephone:</td>
<td><em>Number</em></td>
</tr>
<tr>
<td>Address:</td>
<td><em>Address</em></td>
</tr>
</tbody>
</table>

**BUTIR-BUTIR KAWAN**

<table>
<thead>
<tr>
<th>Name of Kawan:</th>
<th><em>Name</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. Telephone:</td>
<td><em>Number</em></td>
</tr>
</tbody>
</table>

**PENGESYARATAN**

- Saya dengan ini mengesahkan bahawa maklumat yang disebutkan di dalam borang permohonan dan dokumen-dokumen yang diserahkan kepada AMAN DAMAI CAPITAL SDN BHD adalah benar serta tepat. Saya juga diberitahukan bahwa syarikat AMAN DAMAI CAPITAL SDN BHD bertanggungjawab untuk membayar / memeriksa pihak-pihak jika mendapat dokumen-dokumen yang diserahkan adalah tidak benar.
- Tanda tangan: (Cop Jani Kawan)
- Tarihn: ____________

---

**PERINGATAN**

1. Saya serahkan pemberitahuan bahawa saya telah menerima surat tanda terima yang dibimpan oleh Pemegang Papagatai yang dibimbing oleh Aman Damai Capital Sdn Bhd.

---

**BUTIR-BUTIR PEMUNYA**

- No. KP/Pasport: ___________
- Alamat: ___________
- Tanda tangan: ___________

---

**Excessive data collection**

**No consent clause**
Do’s

- Consent clause is incorporated in data collection form.
- Data collection is not excessive and relevant with nature of business
Notice and Choice

Don’ts

- Privacy notice not available on premise/website.
- Privacy notice is placed at inappropriate location such as hallway, not in public’s view.
Do’s

- Client friendly
- Understandable
- Readable
- Accessible to public
Disclosure List

- Consists of all the relevant third parties that company is serving or dealing with in which involves the circulation of clients' personal data.

- Keep track data movement and monitor the third party that handle your data.

- Facilitates investigation and protects your interest.
Appendix V
LIST OF DISCLOSURES
(This Appendix is not intended to be exhaustive but may be amended from time to time as approved by the PDP Commissioner)

<table>
<thead>
<tr>
<th>NO.</th>
<th>THIRD PARTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Financial institutions, merchants, VISA International Services Association, MasterCard International Incorporated and other card associations (in relation to credit cards issue to Data Subject) for the purpose of payment of electricity bill or other services of the Data User</td>
</tr>
<tr>
<td>2.</td>
<td>Postal providers which provide postal services to the Data User</td>
</tr>
<tr>
<td>3.</td>
<td>Telecommunication providers which provides telecommunication services to the Data User</td>
</tr>
<tr>
<td>4.</td>
<td>Service providers which assist the Data User in processing the services that the Data User requested</td>
</tr>
<tr>
<td>5.</td>
<td>Agents/ contractors/ consultants/ vendors/ external auditors/ counsellor/ data processor appointed by the Data User</td>
</tr>
<tr>
<td>6.</td>
<td>Approved bodies where employees contributions are remitted:</td>
</tr>
<tr>
<td></td>
<td>• Social Security Organisation (SOCSO)</td>
</tr>
<tr>
<td></td>
<td>• Baitulmal</td>
</tr>
<tr>
<td></td>
<td>• Pusat Zakat</td>
</tr>
<tr>
<td></td>
<td>• Lembaga Tahung Haji</td>
</tr>
<tr>
<td></td>
<td>• Yayasan Perniagaan Ekonomi Islam Malaysia (YaPEIM)</td>
</tr>
<tr>
<td></td>
<td>• Employees Provident Fund (EPF)</td>
</tr>
<tr>
<td></td>
<td>• Koperasi Wawasan Pekerja-Pekerja Berhad (KOWAJA)</td>
</tr>
<tr>
<td></td>
<td>• Koperasi TNB</td>
</tr>
<tr>
<td></td>
<td>• Insurer/ Broker</td>
</tr>
<tr>
<td>7.</td>
<td>Close family members of Data Subject:</td>
</tr>
<tr>
<td></td>
<td>• Father</td>
</tr>
<tr>
<td></td>
<td>• Mother</td>
</tr>
<tr>
<td></td>
<td>• Husband</td>
</tr>
<tr>
<td></td>
<td>• Wife</td>
</tr>
<tr>
<td></td>
<td>• Siblings</td>
</tr>
</tbody>
</table>

TNB provides a comprehensive disclosure list in the COP
Security

- Documents containing personal data are placed at inappropriate location
- Documents are exposed, not properly kept.
- Malfunctioned CCTV.
- Documents are not properly disposed.
- Passwords to computer log in system are exposed and shared with colleagues.
Do’s

- Access control is well established and practiced.
- ID and Password management is well established and maintained.
- Documents are kept at secure locations/databases.
Retention

Don’ts

- Improper storage of business contracts and financial documents.
- Improper use of storage cabinets.
- No policy on data retention & disposal.
- Cabinets used to store items other than documents.
Do’s

- All documents containing personal data are stored at secure location.
- A good practice of record disposal is well demonstrated
Access Request

Praiseworthy efforts by Public Bank
5. CONCLUSION
1. Identify source of personal data and where those data are located.
2. Govern how personal data is used and accessed.
3. Implement security controls to minimize risk.
4. Establish a Disaster / Incident Response Plan.
Personal Data Governance

Source of Data
- Data subject
- Online
- 3rd party

Storage
- Structured databases
- Physical storage
- Backup system
- Cloud

Usage
- In applications/system
- By employees/marketers
- Shared with 3rd Parties

Retention/Destruction
- Archive
- Destruction

IDENTIFY

PROTECT

CONTROL

PLAN
This presentation is intended to provide general information and guidance on the subject concerned. Any information contained within it may not be reproduced (in whole or in part), copied at any time, used for any purpose other than for your reference without the express written consent from the Personal Data Protection Commissioner Malaysia.