Ref: JPDP.100-1/1/10 (2)
Standard-2015-01.Eng

PERSONAL
DATA PROTECTION
COMMISSIONER MALAYSIA

Ministry of Communication and
Multimedia Malaysia

PERSONAL DATA PROTECTION STANDARD 2015

OFFICE OF THE PERSONAL DATA PROTECTION
COMMISSIONER MALAYSIA
PRECINT 4, LOT 4G9, PERSIARAN PERDANA
FEDERAL GOVERNMENT ADMINISTRATIVE CENTRE
62100 PUTRAJAYA
MALAYSIA

PERSONAL DATA PROTECTION REGULATIONS 2013

PERSONAL DATA PROTECTION STANDARD 2015

PART I

PRELIMINARY

Standard

PERSONAL DATA PROTECTION REGULATIONS 2013

PERSONAL DATA PROTECTION STANDARD 2015

In exercise of the powers conferred by the articles 6,7 and 8 of the Personal Data Protection Regulations 2013 [PU (A) 335], the Commissioner makes the following settings:

PART I

PRELIMINARY

1. **Short title and commencement**

1.1 This Standard may be cited as the Personal Data Protection Standard 2015.

1.2 This Standard comes into operation immediately as of the date published by the Commissioner.

2. **Interpretation**

In this Standard, unless the context otherwise requires-

"standard" means a minimum requirement issued by the Commissioner, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

3. **Application**

3.1 This Standard applies to -

(a) any person who processes; and

(b) any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions.

PART II

PERSONAL DATA PROTECTION STANDARD 2015

Security Standard

4. **Establishment of the security standard for personal data processed electronically.**

4.1 A data user shall, take practical steps to protect the personal data from any loss, misuse, modifications, unauthorized or accidental access or disclosure, alteration or destruction by having regard-

DATA SECURITY FOR PERSONAL DATA PROCESSED ELECTRONICALLY	
No.	**Descriptions**
1.	Register all employees involved in the processing of personal data.
2.	Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organization.
3.	Control and limit employees' access to personal data system for the purpose of collecting, processing and storing of personal data.
4.	Provide user ID and password for authorized employees to access personal data.
5.	Terminate user ID and password immediately when an employee who is authorized access to personal data is no longer handling the data.
6.	Establish physical security procedures as follow: i. control the movement in and out of the data storage site; ii. store personal data in an appropriate location which is unexposed and safe from physical or natural threats;

	iii. provide a closed-circuit camera at the data storage site (if necessary), and iv. provide a 24 hour security monitoring (if necessary).
7.	Update the Back up/Recovery System and anti-virus to prevent personal data intrusion and such.
8.	Safeguard the computer systems from malware threats to prevent attacks on personal data.
9.	The transfer of personal data through removable media device and cloud computing service is not permitted unless with written consent by an officer authorized by the top management of the data user organization.
10.	Record any transfer of data through removable media device and cloud computing service.
11.	Personal data transfer through cloud computing service must comply with the personal data protection principles in Malaysia, as well as with personal data protection laws of other countries.
12.	Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Commissioner.
13.	Ensure that all employees involved in processing personal data always protect the confidentiality of the data subject's personal data.
14.	Bind an appointed third party by the data user with a contract for operating and carrying out personal data processing activities. This is to ensure the safety of personal data from loss, misuse, modification, unauthorized access and disclosure.

5. Establishment of the security standards for personal data processed non-electronically.

5.1 A data user shall, take practical steps to protect the personal data from any loss, misuse, modifications, unauthorized or accidental access or disclosure, alteration or destruction by having regard-

DATA SECURITY FOR PERSONAL DATA PROCESSED NON-ELECTRONICALLY	
No.	**Descriptions**
1.	Register employees handling personal data into a system/registration book before being allowed access to personal data.
2.	Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organization.
3.	Control and limit employees' access to personal data system for the purpose of collecting, processing and storing of personal data.
4.	Establish physical security procedures as follow: i. store all personal data orderly in files; ii. store all files containing personal data in a locked place; iii. keep all the related keys in a safe place; iv. provide record for keys storage; and v. store personal data in an appropriate location which is unexposed and safe from physical or natural threats.
5.	Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Commissioner.
6.	Ensure that all employees involved in processing personal data always protect the confidentiality of the data subject's personal data.

7.	Record personal data transferred conventionally such as through mail, delivery, fax and etc.
8.	Ensure that all used papers, printed documents or other documents exhibiting personal data are destroyed thoroughly and efficiently by using shredding machine or other appropriate methods.
9.	Conduct awareness programmes to all employees (if necessary) on the responsibility to protect personal data.

Retention Standard

6. The standard for retention of personal data which is processed electronically and non-electronically.

6.1 A data user shall, take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed by having regard–

No.	Descriptions
1.	Determine the retention period in all legislation relating to the processing and retention of personal data are fulfilled before destroying the data.
2.	Keep personal data no longer than necessary unless there are requirements by other legal provisions.
3.	Maintain a proper record of personal data disposal periodically and make such record available for submission when directed by the Commissioner.
4.	Dispose personal data collection forms used in commercial transactions within the period not exceeding fourteen (14) days, except if/unless the forms carry legal values in relation to the commercial transaction.
5.	Review and dispose all unwanted personal data that in the database.
6.	Prepare a personal data disposal schedule for inactive data with a 24 month period. The personal data disposal schedule should be maintained properly.
7.	The use of removable media device for storing personal data is not permitted without written approval from the top management of the organization.

Data Integrity Standard

7. Establishment of data integrity standard for personal data processed electronically and non-electronically.

7.1 A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept updated by having regard to the purpose, including any directly related purpose, for which the personal data was collected and processed further. Such measures are:

No.	Descriptions
1.	Provide personal data update form for data subjects, either via online or conventional.
2.	Update personal data immediately once data correction notice is received from data subject.
3.	Ensure that all relevant legislation is fulfilled in determining the type of documents required to support the validity of the data subject's personal data.
4.	Notify on personal data updates either through the portal or notice at premises or by other appropriate methods.

Made 23 DECEMBER 2015
[JPDP.100-1/1/10 (2)]

MAZMALEK BIN MOHAMAD
Personal Data Protection Commissioner
Malaysia