No. Rujukan: JPDP.100-1/1/10 (1)
Standard-2015-01

PESURUHJAYA
PERLINDUNGAN DATA
PERIBADI MALAYSIA

Kementerian Komunikasi
dan Multimedia Malaysia

STANDARD
PERLINDUNGAN DATA PERIBADI 2015

PEJABAT PESURUHJAYA PERLINDUNGAN DATA PERIBADI MALAYSIA
PRESINT 4, LOT 4G9, PERSIARAN PERDANA
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62100 PUTRAJAYA

PERATURAN-PERATURAN PERLINDUNGAN DATA PERIBADI 2013

STANDARD PERLINDUNGAN DATA PERIBADI 2015

BAHAGIAN I

PERMULAAN

Standard

1. Nama dan permulaan kuat kuasa
2. Tafsiran
3. Pemakaian

BAHAGIAN II

STANDARD PERLINDUNGAN DATA PERIBADI

Standard Keselamatan

4. Penetapan Standard Keselamatan Bagi Data Peribadi Yang Diproses Secara Elektronik
5. Penetapan Standard Keselamatan Bagi Data Peribadi Yang Diproses Bukan Secara Elektronik

Standard Penyimpanan

6. Penetapan Standard Penyimpanan Bagi Data Peribadi Yang Diproses Secara Elektronik dan Bukan Secara Elektronik

Standard Integriti Data

7. Penetapan Standard Integriti Data Bagi Data Peribadi Yang Diproses Secara Elektronik dan Bukan Secara Elektronik

PERATURAN-PERATURAN PERLINDUNGAN DATA PERIBADI 2013

STANDARD PERLINDUNGAN DATA PERIBADI 2015

PADA menjalankan kuasa yang diberikan oleh perkara 6,7 dan 8, Peraturan-peraturan Perlindungan Data Peribadi 2013 [P.U. (A) 335], Pesuruhjaya membuat penetapan-penetapan yang berikut:

BAHAGIAN 1

PERMULAAN

1. **Tajuk ringkas dan permulaan kuat kuasa.**

1.1 Standard ini bolehlah dinamakan **Standard Perlindungan Data Peribadi 2015.**

1.2 Standard ini mula berkuatkuasa serta-merta dari tarikh yang disiarkan oleh Pesuruhjaya.

2. **Tafsiran**

Dalam standard ini, melainkan jika konteksnya mengkehendaki makna lain-

"standard' ertinya suatu kehendak minimum yang dikeluarkan oleh Pesuruhjaya, yang memperuntukkan, bagi kegunaan biasa dan berulang, kaedah-kaedah, garis panduan atau ciri-ciri bagi aktiviti atau keputusan aktiviti itu, yang matlamatnya adalah pencapaian peringkat susunan yang optimum dalam sesuatu konteks yang diberikan.

3. **Pemakaian**

3.1 Standard ini terpakai bagi-

(a) mana-mana orang yang memproses; dan

(b) mana-mana orang yang mempunyai kawalan terhadap atau membenarkan pemprosesan apa-apa data peribadi berkenaan dengan transaksi komersil.

BAHAGIAN II

STANDARD PERLINDUNGAN DATA PERIBADI

Standard Keselamatan

4. **Penetapan standard keselamatan bagi data peribadi yang diproses secara elektronik.**

4.1 Pengguna Data hendaklah menyediakan langkah-langkah keselamatan yang praktikal ketika pemprosesan data peribadi untuk melindungi data peribadi itu daripada apa-apa kehilangan, salahguna, ubahsuaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan dengan mengambilkira faktor berikut:

KESELAMATAN DATA PERIBADI SECARA ELEKTRONIK	
Bil.	**Perkara**
1.	Mendaftarkan semua kakitangan yang terlibat dalam pemprosesan data peribadi.
2.	Menamatkan hak akses kakitangan kepada sistem data peribadi selepas kakitangan berhenti kerja, diberhentikan kerja, ditamatkan kontrak atau perjanjian, atau diselaraskan mengikut perubahan dalam organisasi.
3.	Mengawal dan menghadkan takat kuasa kakitangan untuk mengakses data peribadi bagi tujuan mengumpul, memproses dan menyimpan data peribadi.
4.	Menyediakan ID pengguna dan kata laluan untuk kakitangan yang diberi kebenaran mengakses data peribadi.
5.	Membatalkan ID pengguna dan kata laluan dengan serta merta apabila kakitangan yang diberi kebenaran mengakses data peribadi tidak lagi mengendalikan data peribadi.
6.	Menetapkan prosedur keselamatan fizikal seperti yang berikut: i. mengawal pergerakan keluar dan masuk ke tempat penyimpanan data; ii. menyimpan data peribadi di lokasi yang bersesuaian iaitu selamat daripada ancaman fizikal atau semulajadi serta tidak terdedah. iii. menyediakan kamera litar tertutup di tempat penyimpanan data (sekiranya perlu), dan

	iv. menyediakan kawalan keselamatan 24 jam sehari (sekiranya perlu).
7.	Mengemaskini *Back up/Recovery System* dan perisian anti-virus bagi melindungi data peribadi daripada insiden pencerobohan dan sebagainya.
8.	Melindungi sistem komputer daripada ancaman *malware* bagi mengelakkan serangan ke atas data peribadi.
9.	Pemindahan data peribadi melalui peranti media mudah alih *(removable media device)* dan perkhidmatan pengkomputeran awan *(cloud computing service)* adalah tidak dibenarkan **kecuali** dengan kebenaran bertulis pegawai yang diberi kuasa oleh pengurusan tertinggi organisasi pengguna data.
10.	Merekodkan sebarang pemindahan data peribadi yang menggunakan peranti media mudah alih *(removable media device)* dan perkhidmatan pengkomputeran awan *(cloud computing service).*
11.	Pemindahan data peribadi melalui perkhidmatan pengkomputeran awan *(cloud computing service)* perlu mematuhi prinsip-prinsip perlindungan data peribadi di Malaysia dan negara-negara lain yang mempunyai undang-undang perlindungan data peribadi.
12.	Menyelenggara rekod akses ke atas data peribadi secara berkala dengan sempurna dan rekod tersebut hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya.
13.	Memastikan semua kakitangan yang terlibat dalam pemprosesan data peribadi sentiasa menjaga kerahsiaan data peribadi subjek data.
14.	Suatu kontrak perlu diadakan di antara pengguna data dengan pihak yang dilantik oleh pengguna data bagi mengendalikan dan menjalankan aktiviti pemprosesan data peribadi. Ini bagi maksud menjamin keselamatan ke atas data peribadi daripada kehilangan, salah guna, ubah suaian, akses dan penzahiran tanpa kebenaran.

5. **Penetapan standard keselamatan bagi data peribadi yang diproses bukan secara elektronik.**

5.1 Pengguna Data hendaklah menyediakan langkah-langkah keselamatan yang praktikal ketika pemprosesan data peribadi untuk melindungi data peribadi itu daripada apa-apa kehilangan, salahguna, ubahsuaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan dengan mengambil kira faktor berikut:

KESELAMATAN DATA PERIBADI YANG DIPROSES BUKAN SECARA ELEKTRONIK	
Bil.	**Perkara**
1.	Mendaftarkan kakitangan yang menguruskan data peribadi dalam sistem/buku pendaftaran sebelum dibenarkan mengakses data peribadi.
2.	Menamatkan hak akses kakitangan kepada data peribadi selepas kakitangan berhenti kerja, diberhentikan kerja, ditamatkan kontrak atau perjanjian, atau diselaraskan mengikut perubahan dalam organisasi.
3.	Mengawal dan menghadkan takat kuasa mengakses data peribadi bagi tujuan mengumpul, memproses dan menyimpan data peribadi.
4.	Menetapkan prosedur keselamatan fizikal seperti yang berikut: i. menyimpan semua data peribadi secara teratur dalam fail; ii. menyimpan semua fail yang mengandungi data peribadi di tempat yang berkunci**;** iii. menyimpan semua kunci yang berkaitan di tempat yang selamat; iv. menyediakan rekod penyimpanan kunci; dan v. menyimpan data peribadi di lokasi yang bersesuaian iaitu selamat daripada ancaman fizikal atau semulajadi serta tidak terdedah.
5.	Menyelenggara rekod akses ke atas data peribadi secara berkala dengan sempurna dan rekod tersebut hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya.
6.	Memastikan semua kakitangan yang terlibat dalam pemprosesan data peribadi sentiasa menjaga kerahsiaan data peribadi subjek data.

7.	Pemindahan data peribadi secara konvensional seperti melalui pos, serahan tangan, faks dan sebagainya hendaklah direkodkan.
8.	Memastikan semua kertas terpakai, dokumen cetakan atau lain-lain dokumen yang jelas menunjukkan data peribadi perlu dimusnahkan dengan teliti dan efisien seperti menggunakan mesin rincih atau lain-lain kaedah yang bersesuaian.
9.	Mengadakan program kesedaran mengenai tanggungjawab melindungi data peribadi kepada semua kakitangan yang terlibat (sekiranya perlu).

Standard Penyimpanan

6. **Penetapan standard penyimpanan bagi data peribadi yang diproses secara elektronik dan data peribadi yang diproses bukan secara elektronik.**

6.1 Pengguna data mengambil langkah yang munasabah untuk memastikan bahawa segala data peribadi dimusnahkan atau dipadamkan secara kekal. Jika data peribadi itu tidak lagi dikehendaki bagi maksud yang baginya data peribadi itu hendak diproses dengan:

Bil.	Perkara
1.	Menentukan semua perundangan yang berkaitan dengan pemprosesan dan penyimpanan data peribadi dipenuhi sebelum memusnahkan data peribadi.
2.	Tidak menyimpan data peribadi lebih lama daripada yang diperlukan melainkan terdapat peruntukan undang-undang lain yang memerlukan penyimpanan yang lebih lama.
3.	Menyediakan dan menyelenggara rekod pelupusan data peribadi dan rekod tersebut hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya.
4.	Melupuskan borang pungutan data peribadi yang digunakan untuk transaksi komersil dalam tempoh tidak melebihi empat belas (14) hari, melainkan borang tersebut mempunyai nilai perundangan yang berkaitan dengan transaksi komersial tersebut.
5.	Menyemak dan melupuskan semua data peribadi yang tidak diperlukan di dalam pangkalan data.
6.	Mempunyai jadual pelupusan data peribadi yang tidak aktif bagi tempoh 24 bulan. Jadual pelupusan data peribadi tersebut perlu diselenggara dengan sempurna.
7.	Penggunaan peranti media mudah alih *(removable media device)* untuk tujuan penyimpanan data peribadi adalah tidak dibenarkan tanpa kebenaran bertulis daripada pengurusan atasan organisasi.

Standard Integriti Data

7. **Penetapan standard integriti data bagi data peribadi yang diproses secara elektronik dan data peribadi yang bukan diproses secara elektronik.**

7.1 Pengguna data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini dengan mengambilkira maksud, termasuk apa-apa maksud yang berhubungan secara langsung, yang baginya data peribadi itu dikumpulkan dan diproses selanjutnya. Langkah-langkah tersebut adalah:

Bil.	Perkara
1.	Menyediakan borang kemaskini data peribadi untuk diisi oleh subjek data sama ada secara dalam talian atau secara konvensional.
2.	Mengemaskini data peribadi dengan segera setelah mendapat notis pembetulan data peribadi daripada subjek data.
3.	Memastikan semua perundangan berkaitan dipenuhi dalam menentukan jenis dokumen yang diperlukan bagi menyokong kesahihan data peribadi subjek data.
4.	Memaklumkan mengenai pengemaskinian data peribadi sama ada melalui portal atau mempamerkan pemakluman di premis atau dengan lain-lain kaedah yang bersesuaian.

DIKELUARKAN
[JPDP.100-1/1/10 (1)]
[23 DISEMBER 2015]

MAZMALEK BIN MOHAMAD
Pesuruhjaya
Perlindungan Data Peribadi Malaysia

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

1. Short title and commencement

2. Interpretation

3. Application

PART II

PERSONAL DATA PROTECTION STANDARD 2015

Security Standard

4. Establishment of the Security Standard For Personal Data Processed Electronically

5. Establishment of the of Security Standard For Personal Data Processed Non-Electronically

Retention Standard

6. Establishment of the Retention Standard For Personal Data Processed Electronically And Non-Electronically.

Data Integrity Standard

7. Establishment of the Data Integrity Standard For Personal Data Processed Electronically And Non-Electronically.

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 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.	Providing personal data to form update is filled by data subjects whether 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