



14 November 2013
14 November 2013
P.U. (A) 335

WARTA KERAJAAN PERSEKUTUAN

*FEDERAL GOVERNMENT
GAZETTE*

PERATURAN-PERATURAN PERLINDUNGAN DATA
PERIBADI 2013

PERSONAL DATA PROTECTION REGULATIONS 2013



DISIARKAN OLEH/
PUBLISHED BY
JABATAN PEGUAM NEGARA/
ATTORNEY GENERAL'S CHAMBERS

AKTA PERLINDUNGAN DATA PERIBADI 2010
PERATURAN-PERATURAN PERLINDUNGAN DATA PERIBADI 2013

SUSUNAN PERATURAN-PERATURAN

BAHAGIAN I
PERMULAAN

Peraturan

1. Nama dan permulaan kuat kuasa
2. Tafsiran

BAHAGIAN II
PRINSIP PERLINDUNGAN DATA PERIBADI

Prinsip Am

3. Persetujuan subjek data

Prinsip Notis dan Pilihan

4. Perincian tentang pengguna data

Prinsip Penzahiran

5. Senarai penzahiran

Prinsip Keselamatan

6. Polisi keselamatan

Prinsip Penyimpanan

7. Standard penyimpanan

Prinsip Integriti Data

8. Standard integriti data

Prinsip Akses

9. Permintaan mengakses data
10. Keengganan permintaan mengakses data
11. Penerimaan permintaan pembetulan data
12. Penalti

BAHAGIAN III
PEMERIKSAAN

13. Notis pemeriksaan
14. Sistem data peribadi hendaklah terbuka untuk pemeriksaan

BAHAGIAN IV
NOTIS PENGUATKUASAAN

15. Permohonan perubahan atau pembatalan notis penguatkuasaan

AKTA PERLINDUNGAN DATA PERIBADI 2010

PERATURAN-PERATURAN PERLINDUNGAN DATA PERIBADI 2013

PADA menjalankan kuasa yang diberikan oleh seksyen 143 Akta Perlindungan Data Peribadi 2010 [*Akta 709*], Menteri membuat peraturan-peraturan yang berikut:

BAHAGIAN I

PERMULAAN

Nama dan permulaan kuat kuasa

1. (1) Peraturan-peraturan ini bolehlah dinamakan **Peraturan-Peraturan Perlindungan Data Peribadi 2013**.

(2) Peraturan-Peraturan ini mula berkuat kuasa pada 15 November 2013.

Tafsiran

2. Dalam Peraturan-Peraturan ini, melainkan jika konteksnya menghendaki makna yang lain—

“pegawai pemeriksa” ertinya seorang pegawai yang diambil kerja oleh Pesuruhjaya di bawah seksyen 51 Akta bagi maksud menjalankan suatu pemeriksaan di bawah seksyen 101 Akta;

“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.

BAHAGIAN II

PRINSIP PERLINDUNGAN DATA PERIBADI

Prinsip Am

Persetujuan subjek data

3. (1) Seorang pengguna data hendaklah memperoleh persetujuan daripada seorang subjek data berhubung dengan pemprosesan data peribadi dalam apa-apa bentuk yang persetujuan itu boleh direkodkan dan disenggarakan dengan sewajarnya oleh pengguna data itu.

(2) Sekiranya bentuk persetujuan dalam subperaturan (1) yang diberikan melibatkan juga perkara lain, kehendak untuk memperoleh persetujuan hendaklah dikemukakan secara berbeza dalam pengemukaannya daripada perkara lain itu.

(3) Seorang pengguna data hendaklah mendapatkan persetujuan yang disebut dalam subperaturan (1) daripada ibu bapa, penjaga atau seseorang yang mempunyai tanggungjawab ibu bapa terhadap subjek data, sekiranya subjek data itu berumur bawah lapan belas tahun.

(4) Seorang pengguna data hendaklah mendapatkan persetujuan yang disebut dalam subperaturan (1) daripada seseorang yang dilantik oleh mahkamah untuk menguruskan hal-ehwal subjek data atau seseorang yang diberikan kuasa secara bertulis oleh subjek data untuk bertindak bagi pihaknya sekiranya subjek data itu tidak berupaya untuk menguruskan hal-ehwalnya sendiri.

(5) Beban pembuktian bagi persetujuan yang disebut dalam subperaturan (1) hendaklah terletak pada pengguna data.

Prinsip Notis dan Pilihan

Perincian tentang pengguna data

4. Bagi maksud perenggan 7(1)(d) Akta, pengguna data hendaklah sekurang-kurangnya memberikan subjek data perincian seperti yang berikut:

- (a) perjawatan orang yang boleh dihubungi;
- (b) nombor telefon;
- (c) nombor faks, sekiranya ada;
- (d) alamat e-mel, sekiranya ada; dan
- (e) apa-apa maklumat lain yang berkaitan.

Prinsip Penzahiran

Senarai penzahiran

5. Pengguna data hendaklah menyimpan dan menyenggara suatu senarai penzahiran kepada pihak ketiga bagi maksud perenggan 8(b) Akta berhubung dengan data peribadi subjek data yang telah atau sedang diproses olehnya.

Prinsip Keselamatan

Polisi keselamatan

6. (1) Pengguna data hendaklah membangunkan dan melaksanakan suatu polisi keselamatan bagi maksud seksyen 9 Akta.

(2) Pengguna data hendaklah memastikan polisi keselamatan yang disebut dalam subperenggan (1) mematuhi standard keselamatan yang ditetapkan dari semasa ke semasa oleh Pesuruhjaya.

(3) Pengguna data hendaklah memastikan bahawa standard keselamatan dalam memproses data peribadi dipatuhi oleh mana-mana pemproses data yang menjalankan pemprosesan data peribadi bagi pihak pengguna data itu.

Prinsip Penyimpanan

Standard penyimpanan

7. Bagi maksud seksyen 10 Akta, data peribadi seorang subjek data hendaklah disimpan mengikut standard penyimpanan yang ditetapkan dari semasa ke semasa oleh Pesuruhjaya.

Prinsip Integriti Data

Standard integriti data

8. Bagi maksud seksyen 11 Akta, pengguna data hendaklah memproses data peribadi mengikut standard integriti data yang ditetapkan dari semasa ke semasa oleh Pesuruhjaya.

Prinsip Akses

Permintaan mengakses data

9. (1) Jika seorang subjek data tidak menghendaki suatu salinan data peribadi, subjek data hendaklah memaklumkan secara bertulis tentang niatnya kepada pengguna data apabila membuat permintaan mengakses data peribadinya.

(2) Apabila pengguna data menerima permintaan mengakses data daripada subjek data menurut subseksyen 30(2) Akta, pengguna data hendaklah mengakui penerimaan permintaan itu.

Keengganan permintaan mengakses data

10. Bagi maksud perenggan 32(1)(a) dan (b) Akta, “apa-apa maklumat yang dikehendaki dengan munasabah olehnya” ertinya nama, nombor kad pengenalan, alamat dan apa-apa maklumat lain yang berkaitan sebagaimana yang boleh ditentukan oleh Pesuruhjaya.

Penerimaan permintaan pembetulan data

11. Apabila menerima permintaan pembetulan data menurut subseksyen 34(1) Akta, pengguna data hendaklah mengakui penerimaan permintaan itu.

Penalti

12. Mana-mana pengguna data yang melanggar subperaturan 3(1), peraturan 6, 7 dan 8 melakukan kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi dua ratus lima puluh ribu ringgit atau pemenjaraan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

BAHAGIAN III

PEMERIKSAAN

Notis pemeriksaan

13. Pesuruhjaya boleh memberitahu pengguna data secara bertulis tentang niatnya untuk menjalankan pemeriksaan di bawah seksyen 101 Akta.

Sistem data peribadi hendaklah terbuka untuk pemeriksaan

14. (1) Sistem data peribadi hendaklah pada sepanjang masa yang munasabah terbuka untuk diperiksa oleh Pesuruhjaya atau mana-mana pegawai pemeriksa.

(2) Bagi maksud pemeriksaan di bawah seksyen 101 Akta, Pesuruhjaya atau pegawai pemeriksa boleh menghendaki pengemukaan kepadanya—

(a) berhubung dengan prinsip am, rekod persetujuan daripada subjek data yang disenggara berkenaan dengan pemprosesan data peribadi oleh pengguna data;

- (b) berhubung dengan prinsip notis dan pilihan, rekod notis bertulis yang dikeluarkan oleh pengguna data kepada subjek data mengikut seksyen 7 Akta;
- (c) berhubung dengan prinsip penzahiran, senarai penzahiran kepada pihak ketiga bagi maksud perenggan 8(b) Akta berkenaan dengan data peribadi yang telah atau sedang diproses olehnya;
- (d) berhubung dengan prinsip keselamatan, polisi keselamatan yang dibangunkan dan dilaksanakan oleh pengguna data bagi maksud seksyen 9 Akta;
- (e) berhubung dengan prinsip penyimpanan, rekod pematuhan mengikut standard penyimpanan;
- (f) berhubung dengan prinsip integriti data, rekod pematuhan mengikut standard integriti data; atau
- (g) apa-apa maklumat lain yang berkaitan yang disifatkan perlu oleh Pesuruhjaya atau pegawai pemeriksa.

BAHAGIAN IV

NOTIS PENGUATKUASAAN

Permohonan perubahan atau pembatalan notis penguatkuasaan

15. Suatu permohonan perubahan atau pembatalan notis penguatkuasaan oleh pengguna data yang berkaitan kepada Pesuruhjaya di bawah seksyen 109 Akta hendaklah dibuat secara bertulis.

Dibuat 24 Oktober 2013
[KPKK/PUU 800-8/15; PN(PU2)712]

DATO' SRI AHMAD SHABERY CHEEK
Menteri Komunikasi dan Multimedia

PERSONAL DATA PROTECTION ACT 2010

PERSONAL DATA PROTECTION REGULATIONS 2013

ARRANGEMENT OF REGULATIONS

PART I

PRELIMINARY

Regulation

1. Citation and commencement
2. Interpretation

PART II

PERSONAL DATA PROTECTION PRINCIPLES

General Principle

3. Consent of data subject

Notice and Choice Principle

4. Details of data user

Disclosure Principle

5. List of disclosure

Security Principle

6. Security policy

Retention Principle

7. Retention standard

Data Integrity Principle

8. Data integrity standard

Access Principle

9. Data access request
10. Refusal of data access request
11. Receipt of data correction request
12. Penalty

PART III
INSPECTION

13. Notice of inspection
14. Personal data system to be open for inspection

PART IV
ENFORCEMENT NOTICE

15. Application of variation or cancellation of enforcement notice

PERSONAL DATA PROTECTION ACT 2010

PERSONAL DATA PROTECTION REGULATIONS 2013

IN exercise of the powers conferred by section 143 of the Personal Data Protection Act 2010 [*Act 709*], the Minister makes the following regulations:

PART I

PRELIMINARY

Citation and commencement

1. (1) These regulations may be cited as the **Personal Data Protection Regulations 2013**.

(2) These Regulations come into operation on 15 November 2013.

Interpretation

2. In these Regulations, unless the context otherwise requires—

“inspection officer” means an officer employed by the Commissioner under section 51 of the Act for the purposes of carrying out an inspection under section 101 of the Act;

“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.

PART II

PERSONAL DATA PROTECTION PRINCIPLES

General Principle

Consent of data subject

3. (1) A data user shall obtain consent from a data subject in relation to the processing of personal data in any form that such consent can be recorded and maintained properly by the data user.

(2) If the form in which such consent in subregulation (1) is to be given also concerns another matter, the requirement to obtain consent shall be presented distinguishable in its appearance from such other matter.

(3) A data user shall obtain consent referred to in subregulation (1) from the parent, guardian or person who has parental responsibility on the data subject, if the data subject is under the age of eighteen years.

(4) A data user shall obtain consent the consent referred to in subregulation (1) from a person who is appointed by a court to manage the affairs of the data subject or a person authorized in writing by the data subject to act on his behalf if the data subject is incapable of managing his own affairs.

(5) The burden of proof for such consent referred to in subregulation (1) shall lie on the data user.

Notice and Choice Principle

Details of data user

4. For the purposes of paragraph 7(1)(d) of the Act, the data user shall at least provide the data subject the details as follows:

(a) designation of the contact person;

- (b) phone number;
- (c) fax number, if any;
- (d) e-mail address, if any; and
- (e) such other related information.

Disclosure Principle

List of disclosure

5. The data user shall keep and maintain a list of disclosure to third parties for the purposes of paragraph 8(b) of the Act in relation to personal data of the subject data that has been or is being processed by him.

Security Principle

Security policy

6. (1) The data user shall develop and implement a security policy for the purposes of section 9 of the Act.

(2) The data user shall ensure the security policy referred to in subregulation (1) complies with the security standard set out from time to time by the Commissioner.

(3) The data user shall ensure that the security standard in the processing of personal data be complied with by any data processor that carry out the processing of the personal data on behalf of the data user.

Retention Principle

Retention standard

7. For the purposes of section 10 of the Act, the personal data of a data subject shall be retained in accordance with the retention standard set out from time to time by the Commissioner.

Data Integrity Principle

Data integrity standard

8. For the purposes of section 11 of this Act, the data user shall process the personal data in accordance with the data integrity standard set out from time to time by the Commissioner.

Access Principle

Data access request

9. (1) Where a data subject does not require a copy of the personal data, he shall inform the data user in writing of his intention upon making a data access request of his personal data.

(2) Upon receiving the data access request pursuant to subsection 30(2) of the Act, the data user shall acknowledge the receipt of such request.

Refusal of data access request

10. For the purposes of paragraphs 32(1)(a) and (b) of the Act, “such information as he may reasonably require” means name, identification card number, address and such other related information as the Commissioner may determine.

Receipt of data correction request

11. Upon receiving the data correction request pursuant to subsection 34(1) of the Act, the data user shall acknowledge the receipt of such request.

Penalty

12. Any data user who contravenes subregulation 3(1), regulations 6, 7 and 8 commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred and fifty thousand ringgit or imprisonment for a term not exceeding two years or to both.

PART III

INSPECTION

Notice of inspection

13. The Commissioner may notify the data user in writing of his intention to carry out an inspection under section 101 of the Act.

Personal data system to be open for inspection

14. (1) The personal data system shall at all reasonable times be open to the inspection of the Commissioner or any inspection officer.

(2) For the purposes of inspection under section 101 of the Act, the Commissioner or the inspection officer may require the production before him—

- (a) in relation to general principle, the record of the consent from a data subject maintained in respect of the processing of personal data by the data user;
- (b) in relation to notice and choice principle, the record of a written notice issued by the data user to the data subject in accordance with section 7 of the Act;
- (c) in relation to disclosure principle, the list of disclosure to third parties for the purposes of paragraph 8(b) of the Act in respect of personal data that has been or is being processed by him;

- (d) in relation to security principle, the security policy developed and implemented by the data user for the purposes of section 9 of the Act;
- (e) in relation to retention principle, the record of compliance in accordance with the retention standard;
- (f) in relation to data integrity principle, the record of compliance in accordance with the data integrity standard; or
- (g) such other related information which the Commissioner or any inspection officer deems necessary.

PART IV

ENFORCEMENT NOTICE

Application of variation or cancellation of enforcement notice

15. An application of variation or cancellation of enforcement notice by the relevant data user to the Commissioner under section 109 of the Act shall be made in writing.

Made 24 October 2013
[KPKK/PUU 800-8/15; PN(PU2)712]

DATO' SRI AHMAD SHABERY CHEEK
Minister of Communications and Multimedia