KERTAS KONSULTASI AWAM BIL. 04/2024:

STANDARD PERLINDUNGAN DATA PERIBADI

Tarikh Mula : 1 Oktober 2024

Tarikh Tamat : 18 Oktober 2024

BAHAGIAN 1: PENGENALAN DAN LATAR BELAKANG

[A] Pengenalan

1.1 Peraturan-peraturan Perlindungan Data Peribadi 2013 ("**Peraturan**") yang dikeluarkan menurut Akta Perlindungan Data Peribadi 2010 ("**APDP**"), memperuntukkan bahawa Pengawal Data (dan jika berkenaan dengan standard keselamatan, termasuk Pemproses Data juga[1]) hendaklah melaksanakan perkara-perkara berikut[2]:

(a) membangunkan dasar keselamatan menurut **standard keselamatan**;

(b) menyimpan data peribadi menurut **standard penyimpanan**; dan

(c) memproses data peribadi menurut **standard integriti data**,

berdasarkan standard yang ditentukan oleh Pesuruhjaya Perlindungan Data Peribadi ("**Pesuruhjaya**") dari semasa ke semasa.

1.2 Pada 23 Disember 2015, Pesuruhjaya telah mengeluarkan Standard Perlindungan Data Peribadi 2015 ("**Standard"**) menurut Peraturan, yang memperkenalkan satu set **standard keselamatan, penyimpanan dan integriti data** yang menggariskan standard / keperluan pematuhan minimum untuk Prinsip Keselamatan, Prinsip Penyimpanan dan Prinsip Integriti Data yang ditetapkan di bawah APDP.[3] Bahasa dalam Peraturan semasa hanya membenarkan Pesuruhjaya menetapkan standard berhubung dengan **tiga (3) Prinsip Perlindungan Data Peribadi ini.** Oleh itu, tumpuan Kertas Konsultasi Awam ("**KKA**") ini dihadkan kepada cadangan pindaan kepada keperluan **Prinsip Keselamatan, Prinsip Penyimpanan dan Prinsip Integriti Data** sahaja.

1.3 Untuk mematuhi Standard yang ditetapkan, Pengawal Data (dan dalam hal standard keselamatan, Pemproses Data juga) hendaklah mengambil semua langkah yang munasabah untuk memastikan bahawa data peribadi:

(a) dilindungi daripada kehilangan, salah guna, ubah suaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan dengan mengambil kira keperluan **standard keselamatan**;

(b) dimusnahkan atau dipadamkan secara kekal jika ia tidak lagi diperlukan untuk tujuan pemprosesannya dengan mengambil kira keperluan **standard penyimpanan**; dan

(c) tepat, lengkap, tidak mengelirukan dan sentiasa dikemas kini dengan mengambil kira tujuan, termasuk apa-apa tujuan yang berkaitan secara langsung, dengan data

---

[1] Pindaan terkini kepada APDP mengenakan obligasi langsung kepada Pemproses Data untuk mematuhi Prinsip Keselamatan. Oleh itu, Peraturan dan Standard yang berkaitan dengan Prinsip Keselamatan juga akan dikenakan kepada Pemproses Data.

[2] Peraturan 6,7 dan 8.

[3] Penjelasan ringkas mengenai prinsip-prinsip ini adalah seperti berikut: Prinsip Keselamatan (Seksyen 9 APDP) menghendaki Pengawal Data dan Pemproses Data mengambil langkah praktikal untuk melindungi data peribadi daripada apa-apa kehilangan, penyalahgunaan, pengubahsuaian, akses atau penzahiran tanpa kebenaran atau tak sengaja, pengubahan atau pemusnahan; Prinsip Penyimpanan (Seksyen 10 APDP) menghendaki Pengawal Data mengambil langkah yang munasabah untuk memusnahkan atau memadamkan data peribadi secara kekal sebaik sahaja data peribadi tidak lagi diperlukan untuk tujuan ia dikumpulkan; dan Prinsip Integriti Data (Seksyen 11 APDP) menghendaki Pengawal Data mengambil langkah yang munasabah untuk memastikan data peribadi yang dikumpul dan diproses adalah tepat, lengkap, tidak mengelirukan dan dikemas kini.

peribadi yang dikumpulkan dan diproses lebih lanjut, dengan mengamalkan langkah-langkah di bawah **standard integriti data**.

1.4 Untuk memudahkan rujukan, teks penuh keperluan yang ditetapkan di bawah Standard telah dilampirkan dalam **Lampiran 1**.

1.5 Untuk mengemas kini Standard dan menjadikannya selaras dengan amalan terbaik antarabangsa, satu set prinsip keselamatan, prinsip penyimpanan dan prinsip integriti data yang **disemak semula** sedang dibangunkan oleh Pesuruhjaya.

1.6 Selaras dengan perkara di atas, KKA ini bertujuan untuk mengumpulkan pandangan dan maklum balas awam mengenai aspek yang akan atau harus diperjelas dalam cadangan Standard yang disemak semula.

BAHAGIAN 2: CADANGAN PINDAAN KEPADA STANDARD

2.1 Sebagai gambaran keseluruhan, cadangan pindaan kepada Standard dalam Bahagian 2 KKA ini dibahagikan kepada aspek-aspek berikut:

(a) Standard berasaskan hasil;

(b) bahagian yang perlu diperjelaskan di bawah standard keselamatan;

(c) bahagian yang perlu diperjelaskan di bawah standard penyimpanan;

(d) bahagian yang perlu diperjelaskan di bawah standard integriti data; dan

(e) peranan skim pensijilan untuk menunjukkan pematuhan Standard;

[A] Standard berasaskan hasil

2.2 Latar belakang: Standard minimum yang ditetapkan oleh Standard semasa (seperti yang dilampirkan dalam **Lampiran 1**) adalah terdiri daripada peraturan "hitam dan putih", iaitu arahan atau langkah preskriptif dan khusus yang mesti dipatuhi oleh Pengawal Data.

2.3 Contoh peraturan "hitam dan putih" sedemikian yang terkandung dalam Standard termasuk:

(a) keperluan untuk mendaftarkan semua kakitangan yang terlibat dalam pemprosesan data peribadi;

(b) keperluan untuk menamatkan hak akses kakitangan kepada data peribadi selepas peletakan jawatan / penamatan pekerjaan mereka dengan Pengawal Data;

(c) keperluan untuk menyediakan ID pengguna dan kata laluan kepada kakitangan yang diberi kebenaran mengakses data peribadi;

(d) keperluan untuk melupuskan borang pengumpulan data peribadi yang digunakan dalam transaksi komersial dalam tempoh yang tidak melebihi empat belas (14) hari, melainkan borang tersebut mempunyai nilai perundangan yang berkaitan g dengan transaksi komersial tersebut; dan

(e) keperluan untuk merekodkan data peribadi yang dipindahkan secara konvensional seperti melalui pos, serahan tangan, faks dan sebagainya.

2.4 Peraturan "hitam dan putih" sedemikian walaupun memberikan arahan yang preskriptif dan spesifik kepada Pengawal Data untuk menunjukkan pematuhan keperluan Prinsip Keselamatan, Prinsip Integriti Data dan Prinsip Penyimpanan, ianya juga mempunyai kelemahan seperti berikut:

(a) satu set Standard preskriptif tidak mampu menyediakan senarai komprehensif semua langkah yang perlu dilaksanakan oleh Pengawal Data / Pemproses Data untuk melindungi data peribadi atau mematuhi keperluan Prinsip Keselamatan, disebabkan oleh landskap data dan keselamatan yang sentiasa berkembang, ancaman yang muncul dan amalan terbaik yang berkembang;

(b) peraturan “hitam dan putih” gagal mengambil kira tahap langkah berbeza yang harus dilaksanakan oleh Pengawal Data / Pemproses Data, yang sepatutnya bergantung pada risiko yang timbul akibat daripada aktiviti pemprosesan data peribadi yang dijalankan oleh mereka. Sebaliknya, peraturan ini berisiko mengenakan satu set standard / keperluan yang seragam tanpa mengira tahap risiko yang timbul akibat daripada aktiviti pemprosesan data peribadi yang dijalankan oleh Pengawal Data / Pemproses Data;

(c) penguatkuasaan Standard menjadi mencabar kerana Standard semasa hanya menetapkan langkah-langkah keselamatan asas / dasar untuk dipatuhi oleh Pengawal Data, yang tidak sepadan dengan skala atau kerumitan pemprosesan yang dijalankan oleh Pengawal Data / Pemproses Data tertentu. Selanjutnya, peraturan “hitam dan putih” telah menyebabkan kesukaran dalam menguatkuasakan Standard terhadap Pengawal Data dalam hal kegagalan mengambil langkah-langkah keselamatan yang mencukupi untuk mencegah pelanggaran data peribadi, kerana langkah-langkah keselamatan yang diperlukan atau sepatutnya diambil tidak sepadan dengan peraturan preskriptif / spesifik yang digariskan dalam Standard.

2.5 Diperhatikan bahawa bidang kuasa lain secara amnya kurang preskriptif berbanding dengan keperluan yang digariskan dalam Standard dan secara amnya mengelak daripada menetapkan keperluan “hitam dan putih” mengenai langkah-langkah yang perlu dilaksanakan oleh Pengawal Data untuk menunjukkan pematuhan standard keselamatan, integriti data dan penyimpanan yang setara.

2.6 Sebagai contoh, United Kingdom (“**UK**”) tidak menyediakan senarai lengkap langkah keselamatan minimum yang mesti dilaksanakan oleh organisasi untuk memenuhi keperluan keselamatan di bawah Peraturan Umum Perlindungan Data Kesatuan Eropah (“**EU**”) (EU GDPR) / Akta Perlindungan Data UK. Sebaliknya, pihak berkuasa perlindungan data UK menggariskan satu set hasil keselamatan untuk dipatuhi oleh organisasi, dan langkah-langkah yang diambil oleh organisasi untuk mematuhi hasil keselamatan ini adalah berbeza-beza bergantung pada risiko yang diperlihatkan oleh skop dan sifat aktiviti pemprosesan data yang dijalankan oleh organisasi.

2.7 Cadangan: Dicadangkan agar peraturan “hitam dan putih” di bawah Standard digantikan dengan keperluan yang digubal berdasarkan pendekatan yang lebih berasaskan hasil.

2.8 Pendekatan berasaskan hasil akan memberi tumpuan kepada penetapan jangkaan Pesuruhjaya dan hasil yang harus dicapai oleh Pengawal Data, dan beralih daripada menetapkan proses khusus yang harus dilaksanakan oleh Pengawal Data / Pemproses Data.

2.9 Contoh langkah-langkah yang berdasarkan pendekatan berasaskan hasil adalah seperti berikut dan mungkin termasuk langkah-langkah yang ditetapkan di bawah Standard sedia ada:

(a) berkenaan dengan standard keselamatan, terdapat tahap proses dalaman yang sesuai untuk mengurus, menjejaki dan mengehadkan akses kepada data peribadi berdasarkan keperluan mengetahui.

Contoh: menyelenggara senarai inventori pengguna/akaun pengguna dengan akses kepada data peribadi dan memastikan hak akses yang dipegang oleh kakitangan dihapuskan atau dinyahaktif dengan segera jika tidak lagi diperlukan; dan

(b) berkenaan dengan standard keselamatan, Pengawal Data telah melaksanakan langkah-langkah yang boleh dikuatkuasakan di sisi undang-undang untuk mengurus dan mengurangkan risiko keselamatan yang mungkin timbul akibat daripada penggunaan pihak ketiga atau Pemproses Data (cth. pembekal perkhidmatan pihak ketiga yang memproses data peribadi Pengawal Data untuk Pengawal Data)

Contoh: memastikan bahawa Pengawal Data mempunyai perjanjian dengan Pemproses Data yang memerlukan Pemproses Data mengambil langkah-langkah keselamatan yang sewajarnya untuk melindungi data peribadi.

2.10 Walau apa pun perkara di atas, Pesuruhjaya menyedari bahawa perniagaan dan organisasi kecil mungkin kekurangan sumber untuk menentukan cara mematuhi langkah-langkah Standard dan mungkin lebih suka arahan yang jelas mengenai tindakan khusus yang perlu diambil. Dalam hal sedemikian, Pesuruhjaya akan memberikan contoh langkah-langkah praktikal yang boleh dilaksanakan oleh perniagaan dan organisasi kecil untuk memenuhi hasil dan jangkaan yang ditetapkan dan digariskan dalam Standard.

2.11 Sebagai contoh, berhubung dengan keperluan untuk melaksanakan langkah-langkah yang sewajarnya dalam mencegah pendedahan atau kebocoran data peribadi tanpa kebenaran atau tak sengaja oleh kakitangan, Standard akan memberikan contoh seperti menyahaktifkan port USB untuk menyekat apa-apa pemindahan data peribadi melalui peranti mudah alih atau perakam / log percetakan rekod data peribadi, sebagai langkah-langkah yang boleh diambil untuk mematuhi keperluan tersebut. Contoh selanjutnya tentang langkah-langkah yang boleh diterima pakai oleh Pengawal Data / Pemproses Data, boleh didapati dalam **Lampiran 2** di bawah.

2.12 Untuk memastikan Standard diguna pakai berdasarkan risiko yang berkaitan dengan pemprosesan data peribadi, Standard yang dipinda akan menetapkan bahawa pendekatan berasaskan risiko mesti digunakan, dan langkah-langkah yang dilaksanakan untuk memenuhi "hasil" yang ditetapkan mestilah berkadar dengan tahap risiko yang dihadapi oleh organisasi, bergantung pada faktor-faktor seperti:

(a) sifat, skop dan jumlah aktiviti pemprosesan data peribadi; dan

(b) bahaya dan kesan yang mungkin akan berlaku sekiranya terdapat kehilangan, salah guna, ubah suaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan data peribadi.

Soalan 1

Semasa memberikan jawapan anda kepada soalan di bawah, sila berikan justifikasi yang jelas untuk menyokong pandangan anda:

(a) Adakah anda bersetuju dengan pendekatan yang dicadangkan untuk beralih kepada pendekatan berasaskan hasil berdasarkan contoh-contoh yang dinyatakan dalam perenggan 2.9(a) dan (b) di atas yang beralih daripada menetapkan proses tertentu yang perlu dilaksanakan oleh Pengawal Data / Pemproses Data?

(b) Adakah anda meramalkan apa-apa cabaran / kesukaran yang mungkin dihadapi oleh Pesuruhjaya dalam menguatkuasakan standard yang berdasarkan

pendekatan berasaskan hasil? Adakah standard berasaskan hasil terlalu subjektif untuk dikuatkuasakan oleh Pesuruhjaya?

(c) Adakah mana-mana standard keselamatan, integriti data atau penyimpanan bagi sektor khusus sedia ada ditetapkan untuk industri / sektor anda? Jika ya, sila nyatakan.

[B] <u>Bahagian yang perlu diperjelaskan di bawah standard keselamatan</u>

2.13 Latar belakang: Berdasarkan pindaan terkini kepada APDP, Prinsip Keselamatan kini terpakai secara langsung kepada Pengawal Data dan Pemproses Data. Berdasarkan Standard sedia ada, standard keselamatan minimum yang ditetapkan adalah dikategorikan mengikut sama ada data peribadi diproses secara elektronik atau fizikal, yang mungkin bersifat duplikasi.

2.14 Cadangan: Pesuruhjaya mencadangkan untuk menghapuskan pembezaan antara data peribadi yang diproses secara elektronik atau secara fizikal dan menyediakan standard keselamatan yang terpakai kepada data peribadi secara amnya, sama ada ia diproses secara elektronik dan/atau fizikal. Untuk mengelakkan apa-apa kekeliruan yang mungkin, iaitu sama ada sesuatu langkah terpakai kepada data peribadi yang diproses secara elektronik, fizikal atau kedua-duanya, langkah-langkah yang dinyatakan dalam Standard yang dipinda akan, secara lalai, terpakai kepada kedua-dua data peribadi yang diproses secara elektronik dan fizikal. Penekanan atau penjelasan tambahan akan diberikan jika sesuatu langkah hanya terpakai kepada data peribadi yang diproses secara elektronik atau fizikal.

2.15 Untuk menyediakan penyenaraian hasil keselamatan yang lebih komprehensif yang perlu dipenuhi oleh Pengawal Data / Pemproses Data, Pesuruhjaya mencadangkan untuk menjelaskan elemen utama berikut yang berkaitan dengan kawalan keselamatan:

(a) struktur tadbir urus;

(b) kawalan akses;

(c) pengurusan inventori aset dan data;

(d) ancaman digital (cth. perlindungan terhadap virus, perisian hasad dan ancaman lain)

(e) keselamatan rangkaian dan kemas kini perisian;

(f) pengurusan risiko pihak ketiga (cth. menguruskan risiko berkongsi data peribadi dengan Pemproses Data); dan

(g) latihan / kesedaran.

2.16 Sila rujuk kepada **Lampiran 2** di bawah untuk contoh jenis elemen keselamatan, serta langkah keselamatan berkaitan, yang dikenal pasti oleh bidang kuasa lain.

<u>Soalan 2</u>

Semasa memberikan jawapan anda kepada soalan di bawah, sila berikan justifikasi yang jelas untuk menyokong pandangan anda:

(a) Adakah anda bersetuju dengan cadangan penghapusan pembezaan antara langkah keselamatan yang terpakai kepada data peribadi yang diproses secara elektronik atau secara fizikal?

(b) Selain elemen utama yang dirujuk dalam perenggan 2.15 di atas, adakah apa-apa elemen utama tambahan yang anda percaya harus dimasukkan dalam senarai tersebut untuk merangkumi semua hasil keselamatan yang perlu secara menyeluruh?

(c) Adakah anda berpendapat Pengawal Data dan Pemproses Data bersedia untuk melaksanakan langkah-langkah keselamatan yang merangkumi pelaksanaan penyahnamaan dan penggunaan nama samaran bagi data peribadi?

[C] <u>Bahagian yang perlu diperjelaskan di bawah standard penyimpanan</u>

2.17 Latar belakang: Di bawah APDP, Prinsip Penyimpanan hanya terpakai kepada Pengawal Data dan oleh itu, standard penyimpanan minimum yang dibincangkan dalam dokumen ini tidak terpakai secara langsung kepada Pemproses Data. Standard penyimpanan semasa terutamanya meliputi langkah-langkah untuk perancangan tempoh penyimpanan dan penyediaan rekod pelupusan untuk data peribadi.

2.18 Cadangan: Untuk menjadikan langkah-langkah penyimpanan lebih komprehensif, cadangan dibuat untuk memperluaskan lagi langkah-langkah standard penyimpanan dengan merujuk kepada elemen-elemen utama berikut:

(a) tempoh penyimpanan;

(b) dokumentasi dan rekod untuk penyimpanan dan pelupusan data peribadi;

(c) kaedah pemusnahan atau pemadaman data peribadi; dan

(d) penyimpanan data peribadi oleh pihak ketiga.

2.19 Sila rujuk kepada **Lampiran 2** di bawah untuk contoh jenis hasil penyimpanan, serta langkah-langkah penyimpanan berkaitan, yang digunakan oleh bidang kuasa lain.

<u>Soalan 3</u>

Semasa memberikan jawapan anda kepada soalan di bawah, sila berikan justifikasi yang jelas untuk menyokong pandangan anda:

(a) Adakah anda bersetuju dengan cadangan perluasan standard penyimpanan untuk memasukkan elemen utama yang dinyatakan dalam perenggan 2.18 bagi menyediakan garis panduan yang lebih jelas dan komprehensif?

(b) Selain daripada elemen-elemen yang dinyatakan dalam perenggan 2.18, adakah apa-apa elemen utama tambahan atau langkah khusus yang anda percaya harus dimasukkan untuk memperjelas penyimpanan data dengan lebih baik?

[D] Bahagian yang perlu diperjelaskan di bawah standard integriti data

2.20 Latar belakang: Di bawah APDP, Prinsip Integriti Data hanya terpakai kepada Pengawal Data dan tidak terpakai secara langsung kepada Pemproses Data. Penyenaraian semasa standard integriti data minimum adalah ringkas dan tidak memperjelas elemen utama yang berkaitan dengan pengekalan integriti data peribadi. Tambahan, tiada langkah-langkah cukup komprehensif yang perlu diambil oleh Pengawal Data dalam memastikan data peribadi adalah tepat, lengkap, tidak mengelirukan dan sentiasa dikemas kini.

2.21 Cadangan: Untuk memastikan standard integriti data adalah lebih komprehensif, cadangan dibuat untuk memperjelas elemen utama yang berkaitan dengan pengekalan integriti data peribadi serta menunjukkan langkah-langkah integriti data relevan yang boleh diguna pakai oleh Pengawal Data. Pendekatan ini akan menyediakan rangka kerja yang jelas dan terperinci untuk diikuti oleh Pengawal Data, demi memastikan ketepatan, ketekalan dan kebolehpercayaan data peribadi sepanjang kitaran hayatnya.

2.22 Elemen utama yang dicadangkan untuk ditangani berhubung dengan standard integriti data adalah seperti berikut:

(a) pengesahan dan penentusahan data;

(b) pemantauan kualiti data;

(c) ketekalan data (cth., melaksanakan amalan dan prosedur dalaman untuk memastikan data peribadi dikumpulkan dan direkodkan dalam format yang standard dan serasi); dan

(d) pengurusan kitaran hayat data (cth., mengemas kini atau menambah data peribadi baharu dengan segera pada rekod sedia ada yang berkaitan).

2.23 Sila rujuk kepada **Lampiran 2** di bawah untuk contoh jenis hasil integriti data, serta langkah integriti data yang berkaitan, yang digunakan oleh bidang kuasa lain.

Soalan 4

Semasa memberikan jawapan anda kepada soalan di bawah, sila berikan justifikasi yang jelas untuk menyokong pandangan anda:

(a) Adakah anda bersetuju dengan cadangan perluasan standard integriti data untuk memasukkan elemen utama yang dinyatakan dalam perenggan 2.22 di atas demi menyediakan garis panduan yang lebih jelas dan komprehensif?

(b) Adakah apa-apa elemen utama tambahan atau langkah khusus yang anda percaya harus dimasukkan untuk menangani integriti data selain daripada yang dirujuk dalam perenggan 2.22 di atas?

[E] Peranan skim pensijilan untuk menunjukkan pematuhan Standard

2.24 Latar belakang: Standard semasa tidak mengiktiraf secara nyata penggunaan skim pensijilan, tanda atau meterai untuk menunjukkan pematuhan keperluan Standard. Secara amalan, Pengawal Data yang proaktif mungkin telah memperoleh pensijilan privasi data dan sebagainya untuk menunjukkan tahap pematuhan privasi data yang memenuhi atau melebihi keperluan Standard. Oleh itu, di samping pematuhan Standard

yang diperlukan, keperluan pensijilan mungkin merupakan keperluan duplikasi yang tidak perlu untuk Pengawal Data tersebut.

2.25 Pesuruhjaya ambil perhatian bahawa bidang kuasa lain mengiktiraf, menggalakkan atau dengan cara lain menerima penggunaan skim pensijilan, tanda atau meterai sebagai salah satu kaedah yang boleh digunakan oleh Pengawal Data / Pemproses Data untuk menunjukkan pematuhan rangka kerja kawal selia perlindungan data masing-masing.

2.26 Cadangan: Dicadangkan bahawa pensijilan industri diiktiraf sebagai kaedah yang boleh digunakan oleh Pengawal Data / Pemproses Data untuk menunjukkan pematuhan Standard.

2.27 Pensijilan industri adalah bersifat sukarela tetapi digalakkan sebagai cara untuk menunjukkan pematuhan Standard. Walaupun mendapatkan pensijilan industri tidak secara automatik menandakan pematuhan menyeluruh atau kekebalan daripada sanksi atau liabiliti di bawah Standard, ia akan dipertimbangkan oleh Pesuruhjaya sebagai faktor peringanan apabila menilai pematuhan Pengawal Data / Pemproses Data terhadap APDP dan Standard

2.28 Contoh pensijilan industri termasuk pensijilan ISO 27001 untuk Sistem Pengurusan Keselamatan Maklumat (ISMS), pensijilan ISO 27017 bagi kawalan keselamatan maklumat untuk penyediaan dan penggunaan perkhidmatan awan, dan pensijilan ISO 27701 untuk Sistem Pengurusan Maklumat Privasi (PIMS).

<u>Soalan 5</u>

Semasa memberikan jawapan anda kepada soalan di bawah, sila berikan justifikasi yang jelas untuk menyokong pandangan anda:

(a) Adakah pensijilan industri khusus diberi mandat atau disyorkan untuk organisasi dalam sektor anda? Adakah senarai pensijilan yang diluluskan atau diiktiraf dikenakan kepada industri anda? Jika ya, sila nyatakan.

(b) Sila nyatakan jenis pensijilan industri yang harus diiktiraf oleh Pesuruhjaya untuk digunakan oleh Pengawal Data / Pemproses Data sebagai bukti pematuhan Standard?

(c) Apakah cabaran yang mungkin timbul daripada pengiktirafan pensijilan industri untuk kedua-dua Pengawal Data / Pemproses Data, dan bagaimana cabaran ini boleh ditangani?

Lampiran 1

Standard Keselamatan

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 mengehadkan 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 sesuai yang bersesuaian iaitu selamat daripada ancaman fizikal atau semula jadi 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 Sistem Sandaran/ Pemulihan dan perisian anti-virus bagi melindungi data peribadi daripada insiden pencerobohan dan sebagainya.
8	Melindungi sistem komputer daripada ancaman perisian hasad *(malware)* bagi mengelakkan serangan ke atas data peribadi.
9	Pemindahan data peribadi melalui peranti mudah alih dan perkhidmatan pengkomputeran awan adalah tidak dibenarkan kecuali dengan kebenaran bertulis daripada pegawai yang diberi kuasa oleh pengurusan tertinggi organisasi Pengguna Data..
10	Merekodkan apa-apa pemindahan data yang menggunakan peranti media mudah alih dan perkhidmatan pengkomputeran awan.
11	Pemindahan data peribadi melalui perkhidmatan pengkomputeran awan perlu mematuhi prinsip-prinsip perlindungan data peribadi di Malaysia dan undang-undang perlindungan data peribadi negara-negara lain.
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 Pengawal Data dengan pihak yang dilantik oleh Pengawal Data bagi mengendalikan dan menjalankan aktivtiti pemprosesan data peribadi. Ini bagi maksud menjamin keselamatan ke atas data peribadi daripada kehilangan, salah guna, ubah suaian, akses dan penzahiran tanpa kebenaran.

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 mengehadkan takat kuasa mengakses data peribadi bagi tujuan mengumpul, memproses dan menyimpan data peribadi.
4	Menetapkan prosedur keselamatan fizikal seperti 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 sesuai iaitu selamat daripada ancaman fizikal atau semula jadi 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 dengan menggunakan mesin perincih atau lain-lain kaedah yang bersesuaian.
9	Mengadakan program kesedaran mengenai tanggungjawab melindungi data peribadi kepada semua kakitangan yang terlibat (sekiranya perlu).

Standard Penyimpanan

Bil.	Perkara
1	Menentukan semua perundangan yang berkaitan dengan pemprosesan dan penyimpanan data peribadi dipenuhi sebelum memusnahkan data.
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 dalam transaksi komersial 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 dalam pangkalan data.
6	Menyediakan jadual pelupusan data peribadi untuk data yang tidak aktif dalam tempoh 24 bulan. Jadual pelupusan data peribadi tersebut perlu diselenggara dengan sempurna.
7	Penggunaan peranti media mudah alih untuk tujuan penyimpanan data peribadi adalah tidak dibenarkan tanpa kelulusan bertulis daripada pengurusan atasan organisasi.

Standard Integriti Data

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

[baki halaman ini sengaja dibiarkan kosong]

Lampiran 2

*Nota: Untuk mengelakkan keraguan, contoh-contoh yang disediakan di bawah Lampiran 2 ini tidak bertujuan untuk menjadi draf Standard yang disemak semula. Berikut adalah **CONTOH** langkah-langkah keselamatan, penyimpanan, integriti data yang boleh diamalkan oleh Pengawal Data / Pemproses Data untuk menunjukkan pematuhan.*

[A] Contoh Langkah Keselamatan

Elemen utama	Contoh
Tadbir urus	• Terdapat dasar dan proses perlindungan data dan keselamatan maklumat yang sesuai, dan jika perlu, organisasi hendaklah memastikan rekod aktiviti pemprosesan diselenggarakan. • Terdapat langkah-langkah yang sesuai untuk mengenal pasti, menilai dan memahami risiko terhadap keselamatan data peribadi dan sistem yang memproses data ini. • Pengawal Data / Pemproses Data mentakrif, melaksana, menyampai dan menguatkuasa dasar dan proses yang sesuai yang mengarahkan pendekatan keseluruhannya dalam melindungi sistem yang terlibat dalam pemprosesan data peribadi.
Kawalan Akses	• Pengawal Data / Pemproses Data memahami, mendokumentasikan dan mengendalikan akses kepada data peribadi dan sistem yang memproses data ini. • Hak akses yang diberikan kepada pengguna tertentu mesti difahami dan dihadkan kepada pengguna yang secara munasabah memerlukan akses sedemikian untuk melaksanakan tugas mereka, dan dihentikan apabila tidak lagi diperlukan. • Pengawal Data / Pemproses Data menjalankan aktiviti untuk menyemak atau mengesahkan bahawa kebenaran sistem teknikal adalah konsisten dengan hak akses pengguna yang didokumenkan. • Pengawal Data / Pemproses Data harus memastikan bahawa pengguna (atau mana-mana fungsi automatik) yang mengakses data peribadi disahkan dan dibenarkan dengan sewajarnya. • Pengawal Data / Pemproses Data hendaklah menghalang pengguna daripada memuat turun, memindahkan, mengubah atau memadam data peribadi sekiranya tiada sebab yang sah untuk organisasi berbuat demikian. Akses yang sah harus dikekang dengan sewajarnya dan harus ada jejak audit yang sesuai. • Pengawal Data / Pemproses Data harus mempunyai dasar kata laluan yang teguh supaya pengguna tidak mencipta kata laluan yang lemah, seperti yang boleh diteka secara remeh.
Pengurusan inventori aset dan data	• Pengawal Data / Pemproses Data memahami dan mengkatalogkan data peribadi yang diprosesnya dan boleh menerangkan tujuan pemprosesannya. Pengawal Data / Pemproses Data juga memahami risiko yang ditimbulkan kepada Subjek Data daripada apa-apa pemprosesan tanpa kebenaran atau menyalahi undang-undang, kehilangan, kemusnahan atau kerosakan tak sengaja pada data tersebut. • Inventori aset terkini bagi aset organisasi dikekalkan dalam organisasi. • Aset perkakasan dan perisian tanpa kebenaran atau yang telah mencapai tempoh akhir sokongan (EOS) masing-masing hendaklah digantikan. • Langkah-langkah disediakan untuk mengelakkan kebocoran data peribadi tanpa kebenaran / tak sengaja oleh Pengawal Data/Pemproses Data (contohnya penyahnamaan atau penggunaan nama samaran).

Ancaman digital	• Penyelesaian untuk melindungi daripada ancaman digital seperti virus dan perisian hasad hendaklah digunakan dan dipasang untuk melindungi sistem dan rangkaian organisasi. • Kemas kini dan tampung untuk sistem dan aplikasi hendaklah dilaksanakan secepat mungkin.
Risiko pihak ketiga	• Pengawal Data / Pemproses Data memahami dan mengurus risiko keselamatan operasi pemprosesannya yang mungkin timbul akibat menggunakan pihak ketiga sebagai Pemproses Data. Langkah ini termasuk memastikan mereka menggunakan langkah-langkah keselamatan yang sesuai.
Audit dan ujian	• Pengawal Data / Pemproses Data menjalankan ujian berkala untuk menilai keberkesanan langkah-langkah keselamatannya, termasuk pengimbasan virus dan perisian hasad, pengimbasan kerentanan dan ujian penembusan yang sesuai. Keputusan apa-apa ujian hendaklah direkodkan, bersama-sama dengan pelan tindakan pemulihan.
Latihan dan kesedaran	• Pengawal Data / Pemproses Data menyediakan latihan untuk semua pekerja demi memastikan pekerja sedar tentang amalan perlindungan data yang diamalkan oleh Pengawal Data / Pemproses Data dan apa yang diharapkan daripada mereka semasa mengendalikan data peribadi.
Tindak balas insiden	• Perlu ada pelan tindak balas insiden untuk membimbing Pengawal Data / Pemproses Data tentang cara bertindak balas terhadap pelanggaran data peribadi.

[B] <u>Contoh Langkah Penyimpanan</u>

Elemen utama	Contoh
Tempoh penyimpanan	• Pengawal Data mesti mengambil langkah-langkah yang munasabah untuk memusnahkan data peribadi atau memastikan ia dinyahkenalpasti jika data tersebut tidak lagi diperlukan untuk apa-apa tujuan yang mungkin memerlukan penggunaan atau pendedahannya. Obligasi ini dilaksanakan sekiranya tiada keperluan undang-undang lain yang terpakai untuk penyimpanan.
Dokumentasi dan rekod penyimpanan dan pelupusan data peribadi	• Pengawal Data harus mempunyai amalan, prosedur dan sistem untuk mengenal pasti data peribadi yang perlu dimusnahkan atau dinyahkenalpasti. • Pengawal Data harus mengekalkan dokumentasi dan rekod bagi tempoh penyimpanan dan kaedah pelupusan data peribadi.
Kaedah pemusnahan atau pemadaman data peribadi	• Pelupusan melalui pengumpulan sampah atau kitar semula biasanya tidak akan membentuk pengambilan langkah-langkah yang munasabah untuk memusnahkan data peribadi melainkan data tersebut telah dimusnahkan melalui proses seperti pempulpaan, pembakaran, penghancuran, penyepaian atau pencincangan. • Kaedah adalah berbeza-beza bergantung pada jenis perkakasan yang digunakan untuk menyimpan data. Dalam sesetengah kes, anda boleh 'membersihkan' perkakasan untuk mengalih keluar data peribadi yang disimpan dengan sepenuhnya. Sekiranya pemusnahan yang tidak dapat dipulihkan tidak mungkin dijalankan, Pengawal Data harus mengambil langkah-langkah munasabah untuk menyahkenalpasti data. • Apabila tidak mungkin untuk memusnahkan data peribadi yang disimpan dalam format elektronik secara tidak dapat dipulihkan, langkah-langkah munasabah untuk memusnahkannya termasuk meletakkan data 'di luar penggunaan'. Maksudnya: (a) data tidak dapat digunakan atau dizahirkan;

	(b) Pengawal Data tidak boleh memberikan akses data kepada mana-mana entiti lain; (c) data dikelilingi dengan langkah-langkah keselamatan teknikal, fizikal dan organisasi yang sesuai, termasuk kawalan akses, log dan jejak audit; dan (d) Pengawal Data komited untuk mengambil langkah-langkah munasabah untuk memusnahkan data dengan tidak dapat dipulihkan jika atau apabila mungkin dilakukan.
Penyimpanan data peribadi pihak ketiga	• Pada perkakasan pihak ketiga, seperti storan awan, sekiranya Pengawal Data telah mengarahkan pihak ketiga untuk memusnahkan data peribadi dengan tidak dapat dipulihkan, langkah-langkah munasabah termasuk mengesahkan bahawa pemusnahan ini telah dilakukan.

[C] <u>Contoh Langkah Integriti Data</u>

Elemen utama	Contoh
Pengesahan dan penentusahan data	• Jika data peribadi akan digunakan atau dizahirkan untuk tujuan baharu yang bukan tujuan utama pengumpulan data, nilai kualiti data peribadi berkenaan dengan tujuan baharu itu sebelum digunakan atau dizahirkan. • Menghubungi Subjek Data untuk menentusahkan kualiti data peribadi apabila ia digunakan atau dizahirkan, terutamanya jika tempoh yang panjang telah berlalu sejak pengumpulannya.
Pemantauan kualiti data	• Menjalankan semakan secara berkala terhadap kualiti data peribadi yang disimpan oleh organisasi untuk memastikan ia tepat, terkini, lengkap dan relevan pada masa penggunaan atau penzahiran. • Melaksanakan amalan, prosedur dan sistem dalaman untuk mengaudit, memantau, mengenal pasti dan membetulkan data peribadi berkualiti rendah, termasuk memberikan latihan kepada pekerja berkenaan amalan, prosedur dan sistem ini
Ketekalan data	• Melaksanakan protokol untuk memastikan data peribadi dikumpulkan dan direkodkan dalam format yang konsisten.
Pengurusan kitaran hayat data	• Memastikan data peribadi yang dikemas kini atau baharu ditambah dengan segera pada rekod sedia ada yang berkaitan. • Menyediakan cara-cara mudah kepada Subjek Data untuk menyemak dan mengemaskinikan data peribadi mereka secara berterusan. • Mengingatkan Subjek Data untuk mengemas kini data peribadi mereka setiap kali mereka terlibat dengan organisasi. • Memeriksa sama ada pihak ketiga yang telah menyediakan data peribadi telah melaksanakan amalan, prosedur dan sistem yang sesuai untuk memastikan kualiti data.

[baki halaman ini sengaja dibiarkan kosong]