KERTAS KONSULTASI AWAM BIL. 01/2024:

PELAKSANAAN PEMBERITAHUAN PELANGGARAN DATA

BAHAGIAN 1: PENGENALAN DAN LATAR BELAKANG

[A] Pengenalan

1.1 Rang Undang-undang Perlindungan Data Peribadi (Pindaan) 2024 ("**Rang Undang-Undang Pindaan**"), yang memperkenalkan pindaan kepada Akta Perlindungan Data Peribadi 2010 ("**APDP**"), telah diluluskan tanpa pindaan oleh Dewan Rakyat pada 16 Julai 2024, dan oleh Dewan Negara pada 31 Julai 2024. Rang Undang-undang Pindaan itu kini sedang menunggu perkenan Yang di-Pertuan Agong.

1.2 Fasal 6 Rang Undang-undang Pindaan bertujuan untuk memperkenalkan obligasi pemberitahuan pelanggaran data mandatori untuk pengawal data (sebelum ini dikenali sebagai pengguna data)[1] dengan memasukkan Seksyen 12 yang baharu di bawah Bahagian II APDP.

1.3 Untuk memudahkan rujukan, teks penuh Seksyen 12B APDP yang memperuntukkan obligasi pemberitahuan pelanggaran data mandatori adalah seperti berikut:

> ***Pemberitahuan pelanggaran data***
>
> ***12B.*** *(1) Jika seseorang pengawal data mempunyai sebab untuk mempercayai bahawa pelanggaran data peribadi telah berlaku, pengawal data itu hendaklah, dengan secepat yang dapat dilaksanakan, memberitahu Pesuruhjaya mengikut cara dan dalam bentuk yang ditentukan oleh Pesuruhjaya.*
>
> *(2) Jika pelanggaran data peribadi di bawah subseksyen (1) mengakibatkan atau berkemungkinan mengakibatkan apa-apa kemudaratan yang ketara kepada subjek data, pengawal data hendaklah memberitahu pelanggaran data peribadi itu kepada subjek data mengikut cara dan dalam bentuk yang ditentukan oleh Pesuruhjaya tanpa kelengahan yang tidak perlu.*
>
> *(3) Seseorang pengawal data yang melanggar subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi dua ratus lima puluh ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.*

1.4 Lanjutan daripada perkara di atas, istilah "*pelanggaran data peribadi*" ditakrifkan di bawah Fasal 3 Rang Undang-Undang Pindaan seperti berikut:

> *"pelanggaran data peribadi" ertinya apa-apa pelanggaran data peribadi, kehilangan data peribadi, salah guna data peribadi atau akses tanpa kebenaran kepada data peribadi.*

1.5 Bagi melengkapkan obligasi pemberitahuan pelanggaran data yang akan diperkenalkan oleh Seksyen 12B baharu dalam APDP, cadangan Peraturan Perlindungan Data Peribadi (Pemberitahuan Pelanggaran Data Peribadi) ("**Peraturan DBN**") dan Garis Panduan Pemberitahuan Pelanggaran Data Peribadi ("**Garis Panduan DBN**") sedang dibangunkan oleh Pesuruhjaya Perlindungan Data Peribadi ("**Pesuruhjaya**"). Peraturan DBN dan Garis Panduan DBN ini akan menyediakan peruntukan tambahan dan panduan mengenai keperluan pelaksanaan untuk obligasi pemberitahuan pelanggaran data serta melengkapi Seksyen 12B APDP.

[1] Fasal 2 Rang Undang-undang Pindaan menggantikan istilah "pengguna data" dengan "pengawal data" di seluruh Rang Undang-undang Pindaan.

1.6 Selaras dengan perkara di atas, Kertas Konsultasi Awam (“ **KKA** ”) ini adalah bertujuan untuk mengumpul pandangan dan maklum balas orang awam mengenai aspek yang akan atau perlu diperjelaskan dalam Peraturan DBN serta Garis Panduan DBN yang dicadangkan.

BAHAGIAN 2: KEPERLUAN YANG DICADANGKAN UNTUK OBLIGASI PEMBERITAHUAN PELANGGARAN DATA DI BAWAH APDP

2.1 Sebagai gambaran keseluruhan, Bahagian 2 KKA ini adalah mengenai cadangan keperluan yang akan diperjelaskan dalam Peratuan DBN dan Garis Panduan DBN berdasarkan kategori seperti berikut:

(a) Ambang pemberitahuan pelanggaran data kepada Pesuruhjaya;

(b) Ambang pemberitahuan pelanggaran data kepada subjek data yang terjejas;

(c) Kaedah dan bentuk pemberitahuan pelanggaran data kepada Pesuruhjaya;

(d) Kaedah dan bentuk pemberitahuan pelanggaran data kepada subjek data yang terjejas;

(e) Tempoh masa untuk pemberitahuan pelanggaran data kepada Pesuruhjaya;

(f) Tempoh masa untuk pemberitahuan pelanggaran data kepada subjek data yang terjejas;

(g) Pengecualian daripada pemberitahuan pelanggaran data kepada subjek data yang terjejas;

(h) Obligasi kepada pemproses data untuk mematuhi obligasi pemberitahuan pelanggaran data;

(i) Pemakaian serentak rejim pemberitahuan pelanggaran data APDP dengan undang-undang / rejim pemberitahuan pelanggaran sektoral lain; dan

(j) Pengurusan pelanggaran data peribadi dan obligasi penyimpanan rekod.

[A] Ambang pemberitahuan pelanggaran data kepada Pesuruhjaya

2.2 Latar belakang: Untuk memastikan APDP adalah selaras dengan amalan pihak berkuasa perlindungan data dalam bidang kuasa lain (termasuk EU), dicadangkan bahawa obligasi pemberitahuan pelanggaran data kepada Pesuruhjaya di bawah Seksyen 12B(1) APDP dihadkan kepada jenis pelanggaran data peribadi tertentu sahaja yang memenuhi ambang pemberitahuan yang ditetapkan dalam Peraturan DBN dan Garis Panduan DBN.

2.3 Penetapan ambang untuk pemberitahuan pelanggaran data kepada Pesuruhjaya mempunyai dua (2) tujuan utama:

(a) untuk mengelakkan laporan berlebihan mengenai pelanggaran data, dengan itu mengelakkan perbelanjaan yang tidak perlu untuk pengawal data dalam memberi maklum balas dan melaporkan pelanggaran data, dan

(b) untuk mengelakkan Pesuruhjaya daripada menjadi terlebih beban dengan laporan pemberitahuan pelanggaran data peribadi yang kurang kemudaratan serius.

2.4 Cadangan: Adalah dicadangkan bahawa pemberitahuan pelanggaran data yang mandatori di bawah Seksyen 12B APDP kepada Pesuruhjaya dihadkan kepada hanya keadaan di mana:

(a) pelanggaran data peribadi mungkin menyebabkan atau telah menyebabkan *"**kemudaratan yang ketara***"; **ATAU /DAN**

(b) pelanggaran data peribadi itu berkemungkinan atau adalah "***berskala signifikan***".

2.5 Sila ambil perhatian bahawa ambang atau syarat yang digariskan di atas dalam Perenggan 2.4(a) dan 2.4(b) hendaklah dibaca secara bercabang atau bersambung. Dalam erti kata lain, pengawal data dikehendaki memberitahu Pesuruhjaya dan/atau subjek data yang terjejas jika pelanggaran data peribadi memenuhi **salah satu atau kedua-dua** ambang dalam Perenggan 2.4(a) dan 2.4(b).

2.6 Adalah dicadangkan bahawa pelanggaran data peribadi akan dianggap sebagai "*kemudaratan yang ketara*" jika:

(a) akses, pendedahan atau kehilangan data peribadi akibat pelanggaran data peribadi yang mengakibatkan atau berkemungkinan mengakibatkan kecederaan badan, penghinaan, kerosakan kepada reputasi atau perhubungan, kehilangan pekerjaan, peluang perniagaan atau profesional, kehilangan kewangan, kecurian identiti, kesan negatif terhadap rekod kredit subjek data, atau kerosakan atau kehilangan harta benda;

(b) akses, pendedahan atau kehilangan data peribadi yang mengakibatkan atau berkemungkinan mengakibatkan kemudaratan serius kepada subjek data yang terjejas yang mana maklumat tersebut berkaitan, atau telah, sedang atau berkemungkinan besar akan disalahguna untuk tujuan yang menyalahi undang-undang; **ATAU**

(c) data peribadi yang terjejas oleh pelanggaran data peribadi termasuk data peribadi sensitif atau sebarang maklumat lain yang mungkin digunakan untuk membolehkan penipuan identiti seperti nama pengguna, kata laluan atau nombor pengenalan.

2.7 Sebaliknya, pelanggaran data peribadi akan dianggap sebagai "*skala signifikan*" jika bilangan subjek data yang terjejas melebihi atau berkemungkinan melebihi 500 individu.

Soalan 1

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

(a) Apakah pandangan anda tentang rangka kerja yang dicadangkan untuk mengehadkan keperluan pemberitahuan pelanggaran data mandatori kepada Pesuruhjaya di bawah Seksyen 12B(1) dalam APDP kepada hanya pelanggaran data peribadi yang memenuhi ambang yang ditetapkan dalam Perenggan 2.4 di atas?

(b) Adakah anda menganggap ambang 500 subjek data adalah sesuai untuk menentukan bahawa pelanggaran data peribadi adalah "skala signifikan"? Perlukah ia dinaikkan atau diturunkan?

Sebagai rujukan, ambang adalah 500 subjek data yang terjejas di Singapura dan 1,000 subjek data yang terjejas di Jepun.

[B] Ambang pemberitahuan pelanggaran data kepada subjek data yang terjejas

2.8 Latar Belakang: Sama seperti di atas, kami ambil perhatian bahawa dalam bidang kuasa lain, termasuk EU, UK, Singapura dan Indonesia, ambang ditentukan untuk memberitahu subjek data yang terjejas tentang pelanggaran data. Walaupun terdapat sedikit perbezaan dalam ambang ini, unsur kemudaratan muncul sebagai keperluan universal merentas semua bidang kuasa.

2.9 Pendekatan serupa, yang memberi tumpuan kepada unsur kemudaratan kepada subjek data, telah diterima pakai di bawah Seksyen 12B(2) APDP. Seksyen 12B(2) APDP memperuntukkan bahawa pemberitahuan pelanggaran data peribadi kepada subjek data yang terjejas adalah mandatori apabila pelanggaran data peribadi menyebabkan atau mungkin menyebabkan ***"kemudaratan yang ketara"*** kepada subjek data yang terjejas.

2.10 Cadangan: Peraturan DBN dan/atau Garis Panduan DBN akan menjelaskan bahawa pelanggaran data peribadi menyebabkan atau mungkin menyebabkan ***"kemudaratan yang ketara"*** kepada subjek data yang terjejas, jika pelanggaran itu termasuk dalam keadaan yang digariskan dalam Perenggan 2.6 dan Perenggan 2.7 di atas. Dalam hal ini, adalah juga dicadangkan supaya keadaan yang digariskan dalam Perenggan 2.6 dibaca secara bercabang atau bersambung, manakala kriteria yang digariskan dalam Perenggan 2.7 hendaklah dibaca bersambung dengan keadaan yang digariskan dalam Perenggan 2.6.

Contoh:

Pengawal data tidak diperlukan untuk memberitahu subjek data yang terjejas walaupun pelanggaran data peribadi memenuhi semua keadaan yang digariskan di bawah Perenggan 2.6 jika pelanggaran data peribadi tidak memenuhi kriteria yang dinyatakan dalam Perenggan 2.7.

Pengawal data dikehendaki memberitahu subjek data yang terjejas walaupun pelanggaran data peribadi hanya memenuhi satu daripada keadaan yang digariskan di bawah Perenggan 2.6 jika pelanggaran data peribadi memenuhi kriteria yang dinyatakan dalam Perenggan 2.7.

2.11 Untuk memudahkan rujukan, jadual di bawah menetapkan ambang pemberitahuan berbeza yang digunakan untuk pemberitahuan kepada Pesuruhjaya serta pemberitahuan kepada subjek data yang terjejas:

	Pemberitahuan Mandatori kepada Pesuruhjaya	**Pemberitahuan Mandatori kepada Subjek Data Yang Terjejas**
Jika pelanggaran data peribadi berkemungkinan menyebabkan atau telah	✓	✓

	Pemberitahuan Mandatori kepada Pesuruhjaya	Pemberitahuan Mandatori kepada Subjek Data Yang Terjejas
menyebabkan kemudaratan yang signifikan		
Jika pelanggaran data peribadi berkemungkinan atau adalah berskala signifikan	✓	✓

<u>Soalan 2</u>

Apakah pandangan anda tentang skop definisi yang dicadangkan untuk "kemudaratan yang ketara"? Adakah definisinya terlalu luas, atau patutkah ia dihadkan lagi?

[C] <u>Kaedah dan bentuk pemberitahuan pelanggaran data kepada Pesuruhjaya</u>

2.12 <u>Latar Belakang:</u> Sebelum pengenalan rejim pemberitahuan pelanggaran data mandatori melalui Rang Undang-Undang Pindaan, Pesuruhjaya telah menggunakan templat borang pelaporan pelanggaran data ("**Templat Borang Pelaporan**") yang telah digunakan oleh pengawal data untuk melaporkan insiden pelanggaran data peribadi yang menjejaskan organisasi mereka secara sukarela.

2.13 Salinan Templat Borang Pelaporan adalah seperti dalam **Lampiran 1** di bawah.

2.14 Pesuruhjaya memahami bahawa pengawal data mungkin tidak mempunyai semua maklumat yang diminta semasa pelaporan awal pelanggaran data kepada Pesuruhjaya. Oleh itu, Pesuruhjaya tidak mengharapkan pengawal data melengkapkan semua maklumat yang diminta dalam Templat Borang Pelaporan. Pengawal data kemudiannya boleh memberikan butiran atau maklumat lanjut sebaik sahaja ia tersedia berkaitan dengan pelanggaran data peribadi tersebut.

2.15 Pengawal data boleh sama ada menyerahkan Templat Borang Pelaporan yang lengkap dalam salinan cetak kepada pejabat Pesuruhjaya di Putrajaya, atau melalui alamat e-mel khusus Pesuruhjaya untuk pemberitahuan pelanggaran data (iaitu, <u>dbnpdp@pdp.gov.my</u>).

2.16 <u>Cadangan:</u> Pesuruhjaya bercadang untuk mengekalkan Templat Borang Pelaporan semasa untuk melaporkan pelanggaran data oleh pengawal data di bawah Seksyen 12B(1) APDP, dengan kemungkinan pengubahsuaian dibuat pada kandungan dan gaya persembahan Borang Pelaporan Templat.

2.17 Pengubahsuaian yang dicadangkan termasuk memudahkan Templat Borang Pelaporan dengan memasukkan pilihan jatuh turun yang telah ditetapkan untuk menyelaraskan dan menyeragamkan maklum balas yang diperlukan serta mengelakkan soalan bercampur.

2.18 Sebagai contoh, Soalan 2(d) Templat Borang Pelaporan yang diterbitkan semula di bawah untuk kemudahan rujukan kini dibentangkan dalam bentuk bercampur:

Siapakah yang mempunyai akses kepada data, dan bagaimanakah akses diberikan dan dipantau? Adakah terdapat pihak ketiga yang menerima atau memproses data, dan bagaimanakah akses dan penggunaan data pihak ketiga dipantau?

2.19 Soalan ini akan diubah suai untuk membezakan pelbagai jenis maklumat yang diminta dalam soalan-soalan individu.

2.20 Selain itu, Pesuruhjaya juga sedang mempertimbangkan untuk menyediakan alat penilaian kendiri untuk membantu pengawal data untuk menentukan sama ada pelanggaran data peribadi perlu dilaporkan, serta menubuhkan saluran bantuan khas untuk menawarkan panduan kepada pengawal data.

Soalan 3

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

(a) Adakah terdapat sebarang bahagian maklumat dalam Templat Borang Pelaporan semasa yang perlu ditambah, atau dibuang (contoh, jika soalan itu mungkin terlalu teknikal / sukar untuk sesetengah pengawal data, atau maklumat itu boleh diminta kemudian oleh Pesuruhjaya semasa proses siasatannya)?

Untuk tujuan ilustrasi, maklumat yang diminta di bawah Soalan 4 (mengenai langkah-langkah/kawalan keselamatan sedia ada yang dilaksanakan oleh pengawal data) mungkin terlalu teknikal untuk kategori pengawal data tertentu, dan boleh diminta kemudian oleh Pesuruhjaya berdasarkan kes demi kes.

(b) Adakah anda fikir penggantian soalan tertentu dengan pilihan jatuh turun yang telah ditetapkan untuk jawapan akan membantu untuk memperkemas dan memudahkan pengawal data untuk melengkapkan Templat Borang Pelaporan?

(c) Sebagai pengawal data, pernahkah anda menghadapi atau menjangkakan sebarang cabaran atau kesukaran mungkin dihadapi dalam melengkapkan Templat Borang Pelaporan dan menyerahkan pemberitahuan pelanggaran data kepada Pesuruhjaya melalui saluran pemberitahuan yang dinyatakan dalam Perenggan 2.15 di atas?

(d) Adakah anda fikir JPDP harus terus membenarkan penyerahan pemberitahuan pelanggaran data dalam salinan fizikal atau cetak, dengan mengambil kira bahawa perniagaan kecil mungkin tidak mempunyai kemahiran teknologi untuk menyerahkan pemberitahuan pelanggaran data melalui saluran elektronik atau dalam talian?

(e) Adakah anda fikir bahawa alat penilaian kendiri atau saluran bantuan khas akan bermanfaat dalam membantu pengawal data dalam menentukan sama ada pelanggaran data peribadi perlu diberitahu?

(f) Pada pendapat anda, apakah penambahbaikan lain yang boleh dilakukan terhadap Templat Borang Pelaporan atau proses pemberitahuan kepada Pesuruhjaya secara amnya?

[D] Cara dan bentuk pemberitahuan pelanggaran data kepada subjek data yang terjejas

2.21 Latar Belakang: Bidang kuasa lain secara umumnya mengamalkan pendekatan yang lebih fleksibel dalam kaedah dan bentuk pemberitahuan pelanggaran data yang diperlukan kepada subjek data yang terjejas, berbanding dengan pemberitahuan kepada pihak berkuasa perlindungan data.

2.22 Walau bagaimanapun, bidang kuasa ini masih menetapkan maklumat minimum yang perlu diberikan apabila pengawal data membuat pemberitahuan kepada subjek data. Jenis maklumat minimum yang ditetapkan biasanya tidak sebanyak maklumat yang diperlukan untuk pemberitahuan kepada pihak berkuasa perlindungan data.

2.23 Ini kerana tujuan utama pemberitahuan kepada subjek data yang terjejas adalah untuk memaklumkan mereka tentang potensi risiko yang mungkin terhasil daripada pelanggaran data peribadi yang menjejaskan pengawal data dan untuk memberikan maklumat tentang langkah pencegahan yang boleh diambil oleh subjek data untuk mengurangkan risiko tersebut.

2.24 Cadangan: Adalah dicadangkan bahawa pengawal data dikehendaki menyediakan, sekurang-kurangnya, maklumat berikut apabila memberitahu subjek data yang terjejas tentang pelanggaran data peribadi:

(a) Penerangan mengenai pelanggaran data peribadi yang telah berlaku;

(b) Butiran mengenai data peribadi yang telah dikompromi atau terjejas oleh pelanggaran data peribadi;

(c) Akibat atau kemudaratan yang mungkin timbul akibat daripada pelanggaran data peribadi;

(d) Penerangan mengenai langkah-langkah yang telah atau akan diambil oleh pengawal data untuk menangani / mengawal pelanggaran data peribadi;

(e) Cadangan mengenai langkah-langkah / tindakan yang boleh diambil oleh subjek data yang terjejas sebagai tindak balas kepada pelanggaran data peribadi; dan

(f) Sediakan butiran pegawai perhubungan di mana maklumat lanjut tentang pelanggaran data boleh diperolehi (contohnya, butiran pegawai perlindungan data pengawal data).

2.25 Selain itu, adalah juga dicadangkan bahawa pengawal data dikehendaki memberitahu / menyampaikan pelanggaran data peribadi kepada subjek data yang terjejas secara langsung (contoh, melalui pemberitahuan e-mel terus kepada subjek data), melainkan jika berbuat demikian akan melibatkan usaha yang tidak seimbang. Dalam kes ini, komunikasi / kenyataan awam atau langkah-langkah yang serupa adalah mencukupi.

2.26 Garis Panduan DBN akan memberikan contoh lanjut mengenai saluran komunikasi yang boleh diguna pakai / digunakan oleh pengawal data untuk memberitahu subjek data tentang sebarang pelanggaran data peribadi yang menjejaskan data peribadi mereka.

Soalan 4

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

(a) Apakah pandangan anda tentang senarai cadangan maklumat minimum yang mesti disediakan oleh pengawal data kepada subjek data yang terjejas? Adakah terdapat sebarang jenis maklumat tambahan yang anda percaya perlu disertakan dalam pemberitahuan kepada subjek data yang terjejas? Jika ya, sila nyatakan.

(b) Adakah anda menjangkakan sebarang cabaran atau halangan untuk pengawal data dalam menyediakan maklumat minimum yang dicadangkan kepada subjek data yang terjejas? Jika ya, sila huraikan.

(c) Bagaimanakah proses memaklumkan subjek data yang terjejas boleh dipercekapkan dan kurang membebankan pengawal data, terutamanya untuk Perusahaan Kecil dan Sederhana (PKS)?

(d) Apakah pandangan anda tentang cadangan untuk menggunakan komunikasi / kenyataan awam sebagai kaedah pemberitahuan alternatif apabila komunikasi langsung akan melibatkan usaha yang tidak seimbang? Adakah terdapat kaedah alternatif lain yang perlu dipertimbangkan?

[E] Tempoh masa untuk pemberitahuan pelanggaran data kepada Pesuruhjaya

2.27 Latar Belakang: Dari segi tempoh masa untuk pemberitahuan pelanggaran data peribadi kepada pihak berkuasa perlindungan data, bidang kuasa lain biasanya memerlukan pemberitahuan dalam tempoh tujuh puluh dua (72) jam (atau tiga (3) hari kalendar, seperti di Singapura) dari masa pengawal data "menyedari" pelanggaran data tersebut.

2.28 Cadangan: Berkenaan dengan tempoh masa pemberitahuan kepada Pesuruhjaya, adalah dicadangkan bahawa pengawal data mesti memberitahu Pesuruhjaya tidak lewat daripada tujuh puluh dua (72) jam selepas pengawal data menyedari berlakunya pelanggaran data. Ini akan sejajar dengan tempoh masa pemberitahuan pelanggaran data yang diterima pakai oleh bidang kuasa lain, termasuk EU.

2.29 Pengawal data dianggap telah "menyedari" pelanggaran data apabila terdapat tahap kepastian yang munasabah bahawa pelanggaran data telah berlaku dan yang telah menyebabkan data peribadi dikompromi. Pengawal data boleh dikatakan mempunyai tahap kepastian yang munasabah jika terdapat bukti yang mencukupi yang menunjukkan bahawa pelanggaran data peribadi telah berlaku.

2.30 Sebagai contoh, pengawal data dianggap telah menyedari pelanggaran data peribadi apabila pihak ketiga memberitahu mereka bahawa mereka telah salah menerima data peribadi salah seorang pelanggan pengawal data dan memberikan bukti pendedahan tanpa kebenaran. Selain itu, pengawal data akan dianggap telah menyedari jika ia menerima pemberitahuan daripada pemproses datanya bahawa terdapat bukti pelanggaran data peribadi.

2.31 Panduan dan penjelasan lanjut akan disediakan dalam Garis Panduan DBN untuk membantu pengawal data menentukan masa mereka akan dianggap telah "menyedari"

pelanggaran data, yang akan memulakan tempoh masa 72 jam di mana pengawal data mesti menilai sama ada pelanggaran data mesti diberitahu kepada Pesuruhjaya.

Soalan 5

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

(a) Adakah anda fikir pengiraan masa untuk jangka masa 72 jam dari masa pengawal data "menyedari" adalah jelas, atau mungkinkah ia berpotensi menyebabkan kekeliruan kepada pengawal data?

(b) Apakah pandangan anda tentang garis masa yang dicadangkan untuk pemberitahuan pelanggaran data kepada Pesuruhjaya?

(c) Adakah anda fikir garis masa yang dicadangkan untuk pemberitahuan pelanggaran data kepada Pesuruhjaya mengimbangi keperluan untuk pemberitahuan segera dengan kepraktisan mengurus pelanggaran data? Jika tidak, bolehkah anda berikan contoh yang jelas bagaimana garis masa mungkin sukar dipatuhi untuk pengawal data dalam sektor anda?

[F] Tempoh masa untuk pemberitahuan pelanggaran data kepada subjek data yang terjejas

2.32 Latar belakang: Di bidang kuasa lain, tempoh masa untuk memberitahu subjek data yang terjejas biasanya lebih fleksibel berbanding dengan tempoh masa pemberitahuan kepada pihak berkuasa perlindungan data mengenai pelanggaran data peribadi. Secara umumnya, ia ditetapkan bahawa pemberitahuan harus dibuat tanpa kelewatan yang tidak wajar, pada masa yang sama dengan pemberitahuan kepada pihak berkuasa perlindungan data, atau secepat mungkin selepas itu.

2.33 Cadangan: Seksyen 12B(2) APDP memerlukan pengawal data untuk memberitahu subjek data yang terjejas "tanpa kelengahan yang tidak perlu". Dalam hal ini, Garis Panduan DBN dicadang menjelaskan "tanpa kelengahan yang tidak perlu" adalah bermaksud pengawal data mesti memberitahu subjek data pada masa yang sama dengan pemberitahuan kepada Pesuruhjaya, atau secepat mungkin selepas itu.

Soalan 6

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

(a) Apakah pandangan anda tentang garis masa yang dicadangkan untuk pemberitahuan pelanggaran data kepada subjek data yang terjejas?

(b) Adakah anda fikir garis masa yang dicadangkan untuk pemberitahuan pelanggaran data kepada subjek data yang terjejas mencukupi untuk mengimbangi keperluan untuk pemberitahuan segera dengan kepraktisan mengurus pelanggaran data? Jika tidak, bolehkah anda berikan contoh yang jelas bagaimana garis masa mungkin sukar dipatuhi untuk pengawal data dalam sektor anda?

[G] Pengecualian daripada pemberitahuan pelanggaran data kepada subjek data

2.34 Latar Belakang: Rejim pemberitahuan pelanggaran data di bidang kuasa lain, termasuk EU, UK, Jepun, Singapura dan New Zealand, mengecualikan atau membenarkan pengawal data menangguhkan pemberitahuan kepada subjek data yang terjejas dalam keadaan tertentu, contohnya apabila tindakan telah diambil oleh pengawal data untuk memastikan bahawa risiko atau kemudaratan kepada subjek data yang terjejas tidak akan berlaku lagi.

2.35 Cadangan: Adalah dicadangkan agar pengawal data dikecualikan atau dibenarkan untuk menangguhkan pemberitahuan pelanggaran data kepada subjek data yang terjejas dalam keadaan berikut:

(a) pengawal data telah melaksanakan langkah-langkah perlindungan teknologi dan organisasi yang sesuai yang menjadikan pelanggaran itu tidak mungkin mengakibatkan kemudaratan yang ketara kepada subjek data yang terjejas;

(b) data peribadi yang dikompromi atau terjejas oleh pelanggaran dilindungi oleh satu atau lebih langkah-langkah keselamatan yang menjadikan maklumat itu tidak dapat difahami atau tidak bermakna kepada mana-mana individu yang tidak diberi kuasa untuk mendapatkan maklumat tersebut; atau

(c) apabila Pesuruhjaya mengarahkan sebaliknya.

2.36 Adalah dicadangkan bahawa pengawal data tidak perlu mendapatkan kelulusan terlebih dahulu daripada Pesuruhjaya untuk pengecualian atau penangguhan pemberitahuan kepada subjek data yang terjejas.

2.37 Walau bagaimanapun, pengawal data akan dikehendaki menyatakan dalam Borang Pelaporan Templat, apabila memberitahu Pesuruhjaya, sama ada mereka merancang untuk memberitahu subjek data yang terjejas tentang pelanggaran data dan memberikan justifikasi mereka untuk tidak memberitahu atau menangguhkan pemberitahuan kepada subjek data yang terjejas .

2.38 Pesuruhjaya, atas penyiasatan dan penilaiannya sendiri, boleh mengarahkan pengawal data untuk memberitahu subjek data yang terjejas tentang pelanggaran data jika Pesuruhjaya tidak bersetuju dengan justifikasi yang diberikan oleh pengawal data.

Soalan 7

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

(a) Apakah pandangan anda tentang cadangan pengecualian / alasan penangguhan pemberitahuan kepada Subjek Data yang terjejas? Adakah anda percaya terdapat sebarang keadaan tambahan di mana pengecualian atau penangguhan harus dipertimbangkan? Jika ya, sila nyatakan dan berikan justifikasi.

(b) ***Berdasarkan pengalaman anda, apakah faktor yang boleh melambatkan pemberitahuan kepada subjek data yang terjejas, dan bagaimanakah perkara ini boleh ditangani dalam Garis Panduan DBN?***

[H] Obligasi pemproses data untuk mematuhi obligasi pemberitahuan pelanggaran data

2.39 Latar Belakang: Rejim pemberitahuan pelanggaran data di bidang kuasa lain, contohnya, di EU dan Singapura, mengenakan obligasi ke atas pemproses data (dan setara dengannya) untuk memberitahu pengawal data mereka jika terdapat sebab untuk mempercayai bahawa pelanggaran data peribadi telah berlaku. Ini membolehkan pengawal data menilai dan mematuhi keperluan pemberitahuan pelanggaran data di bawah undang-undang perlindungan data masing-masing.

2.40 Cadangan: Adalah dicadangkan bahawa Peraturan DBN dan/atau Garis Panduan DBN menetapkan keperluan bagi pengawal data untuk mengenakan obligasi ke atas pemproses data mereka secara kontrak untuk memberitahu mereka dengan segera tentang pelanggaran data peribadi yang telah berlaku, dan untuk menyediakan semua bantuan yang munasabah dan perlu kepada pengawal data untuk memenuhi obligasi pemberitahuan pelanggaran data pengawal data di bawah APDP dan Garis Panduan DBN.

2.41 Dicadangkan bahawa Garis Panduan DBN membenarkan fleksibiliti untuk pengawal data untuk menentukan tempoh masa tertentu untuk pemberitahuan / pelaporan pelanggaran data peribadi kepada perhatian pengawal data, dengan syarat tempoh masa tersebut dapat menyokong pengawal data dalam memenuhi obligasi pemberitahuan pelanggaran datanya untuk kedua-dua Pesuruhjaya dan subjek data yang terjejas.

2.42 Jika pemproses data menyediakan perkhidmatan kepada berbilang pengawal data yang semuanya terjejas oleh insiden pelanggaran data peribadi yang sama, pemproses data mesti melaporkan butiran kejadian secara berasingan kepada setiap pengawal data.

Soalan 8

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

(a) Apakah pandangan anda tentang cadangan untuk mewajibkan pengawal data mengikat pemproses data mereka secara kontrak untuk memberitahu mereka tentang pelanggaran data peribadi yang telah berlaku?

(b) Adakah perlu untuk menetapkan tempoh masa tertentu di mana pemproses data mesti memberitahu pengawal data tentang kemungkinan pelanggaran data? Jika ya, apakah tempoh masa yang sesuai (cth, dalam masa 24 jam)?

(c) Berdasarkan pengalaman anda, apakah cabaran atau isu yang mungkin timbul daripada keperluan yang dicadangkan untuk pemproses data untuk memberitahu pengawal data, dan bagaimanakah perkara ini boleh ditangani dalam Garis Panduan DBN?

[I] Pemakaian serentak rejim pemberitahuan pelanggaran data apdp dengan undang-undang lain / rejim pemberitahuan pelanggaran sektor

2.43 Latar Belakang: Selain daripada obligasi pemberitahuan pelanggaran data di bawah APDP, pengawal data mungkin dikehendaki memberitahu pihak berkuasa kawal selia lain yang berkaitan tentang pelanggaran data peribadi, jika berkenaan.

2.44 Ini mungkin termasuk keperluan pemberitahuan seperti yang ditetapkan dalam Akta Keselamatan Siber, Dokumen Dasar Bank Negara Malaysia mengenai Pengurusan Maklumat Pelanggan dan Pendedahan Dibenarkan dan Garis Panduan Pengurusan Risiko Teknologi Suruhanjaya Sekuriti Malaysia (yang akan menggantikan Garis Panduan Pengurusan Risiko Siber pada 1 Ogos 2024).

2.45 Kami ambil perhatian bahawa rejim pemberitahuan pelanggaran data peribadi di bidang kuasa lain (contohnya, EU dan Singapura) beroperasi secara berasingan dan serentak dengan keperluan pemberitahuan pelanggaran data lain yang berkenaan yang dikenakan di bawah undang-undang mereka. Pengawal data dikehendaki menjalankan penilaian berasingan untuk menentukan sama ada mereka perlu mematuhi obligasi pemberitahuan berbeza yang dikenakan oleh pengawal selia yang berbeza, dan menyerahkan pemberitahuan pelanggaran data berasingan kepada pengawal selia yang berbeza jika berkenaan.

2.46 Pendekatan untuk pemberitahuan berasingan ini diperlukan kerana ambang pemberitahuan dan keperluan berbeza-beza mengikut peraturan yang berbeza. Selain itu, setiap pengawal selia mempunyai mandat kawal selia yang berbeza dan menumpukan kepada aspek yang berbeza apabila menyiasat pelanggaran data.

2.47 Cadangan: Adalah dicadangkan bahawa Peraturan DBN dan/atau Garis Panduan DBN menjelaskan bahawa obligasi pemberitahuan pelanggaran data di bawah APDP tidak mengatasi sebarang obligasi pemberitahuan yang berkenaan kepada pengawal selia lain atau di bawah mana-mana undang-undang / peraturan lain di Malaysia.

2.48 Ini bermakna pengawal data dikehendaki membuat penilaian berasingan sama ada insiden pelanggaran data berada dalam ambang pemberitahuan yang ditetapkan di bawah peraturan berbeza yang mungkin terpakai kepada mereka, termasuk APDP dan peraturan sektor lain, serta mengemukakan pemberitahuan berasingan kepada pengawal selia yang berkaitan berdasarkan penilaian mereka.

Soalan 9

Adakah terdapat sebarang peraturan lain yang terpakai untuk perniagaan / sektor anda yang mengenakan keperluan pemberitahuan pelanggaran data yang serupa untuk pengawal data atau organisasi secara umum dalam sektor anda? Sila berikan penjelasan ringkas tentang keperluan yang berkenaan.

[J] Pengurusan pelanggaran data peribadi dan obligasi penyimpanan rekod

2.49 Latar Belakang: Selain menggariskan obligasi pengawal data dan pemproses data dalam memberitahu pihak berkuasa perlindungan data dan subjek data yang terjejas tentang pelanggaran data peribadi, bidang kuasa lain juga menyediakan panduan tentang langkah-langkah yang mesti diambil oleh pengawal data untuk bertindak balas, membendung dan mengurus pelanggaran tersebut.

2.50 Selain itu, terdapat juga obligasi penyimpanan rekod yang digariskan bagi pengawal data untuk mendokumenkan pelanggaran data peribadi yang telah menjejaskan organisasi mereka serta langkah-langkah yang diambil untuk memberi maklum balas dan membendung pelanggaran data peribadi.

2.51 Cadangan: Dicadangkan bahawa Garis Panduan DBN menjelaskan dan menyediakan panduan tentang amalan terbaik untuk pengawal data tentang cara bertindak balas

secara berkesan terhadap pelanggaran data, menyiasat dan membendungnya, serta melaksanakan langkah-langkah untuk mencegah berulangnya pelanggaran serupa pada masa hadapan.

2.52 Selain itu, dicadangkan bahawa Garis Panduan DBN juga memperkenalkan keperluan bagi pengawal data untuk membangunkan dan melaksanakan pelan pengurusan pelanggaran data bagi memastikan mereka dapat bertindak balas dengan segera terhadap sebarang pelanggaran data peribadi. Garis Panduan DBN akan menggariskan senarai minimum perkara atau komponen yang mesti ditangani dalam pelan pengurusan pelanggaran data.

2.53 Dari segi obligasi penyimpanan rekod pengawal data, adalah dicadangkan bahawa pengawal data dikehendaki mendokumenkan dan mengekalkan rekod yang betul bagi semua pelanggaran data peribadi, tidak kira sama ada pelanggaran data itu diberitahu kepada Pesuruhjaya dan/atau subjek data yang terjejas.

<u>Soalan 10</u>

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

(a) Apakah pandangan anda tentang jenis amalan terbaik yang harus disyorkan untuk pengawal data apabila menilai, membendung, mengurangkan dan mencegah pelanggaran data peribadi yang serupa daripada berlaku pada masa hadapan? Adakah terdapat amalan khusus yang anda percaya penting untuk pengurusan pelanggaran data peribadi yang berkesan?

(b) Adakah anda bersetuju dengan cadangan untuk memerlukan pengawal data untuk membangunkan dan melaksanakan pelan pengurusan pelanggaran data? Apakah komponen utama yang anda percaya perlu disertakan dalam pelan ini untuk memastikan pengurusan pelanggaran data yang berkesan?

(c) Dari segi obligasi penyimpanan rekod yang dicadangkan, apakah unsur utama atau jenis maklumat yang anda fikir mesti dimasukkan dalam rekod pengawal data untuk memastikan dokumentasi komprehensif untuk pelanggaran data peribadi?

(d) Berdasarkan pengalaman anda, apakah cabaran biasa yang dihadapi oleh pengawal data dalam mematuhi keperluan pemberitahuan pelanggaran data, serta dalam mengambil langkah-langkah untuk membendung dan mengurangkan pelanggaran data peribadi?

Lampiran 1 – Templat Borang Pelaporan

PERSONAL
DATA PROTECTION
COMMISSIONER MALAYSIA
Ministry of Communications
and Digital

PEMBERITAHUAN PELANGGARAN DATA

Templat pemberitahuan ini perlu digunakan apabila pengawal data ingin melaporkan pelanggaran data peribadi yang telah berlaku atau mungkin berlaku dalam organisasi, dalam keadaan di mana pelanggaran tersebut menimbulkan risiko kepada subjek data yang terjejas. Apabila melengkapkan borang ini, jangan sertakan sebarang data peribadi yang terlibat dalam pelanggaran tersebut. Sila ambil perhatian bahawa templat notifikasi ini bukanlah lengkap sepenuhnya. Pesuruhjaya mungkin memerlukan butiran lanjut mengenai insiden tersebut untuk membantu siasatan.

BUTIR-BUTIR PENGAWAL DATA DAN INDIVIDU YANG MEMBERIKAN PEMBERITAHUAN INI

Organisasi : ----------

Alamat : ----------

Individu untuk dihubungi

Nama :

Jawatan :

Nombor Telefon : **Faks :**

E-mel :

Tarikh :

Tandatangan
:

Berdasarkan maklumat yang anda berikan, kami akan menghubungi anda untuk memaklumkan langkah seterusnya. Semua data peribadi yang dikemukakan hanya akan digunakan bagi tujuan yang berkaitan secara langsung dengan pemberitahuan ini, pelaksanaan kuasa dan fungsi pengawalseliaan Pesuruhjaya.

Penyerahan pemberitahuan:

PESURUHJAYA PERLINDUNGAN DATA PERIBADI, MALAYSIA
6 th Floor, Lot 4G9, Kompleks Kementerian Komunikasi & Digital
Persiaran Perdana, Presint 4,
62100 Putrajaya
atau melalui e-mel: dbnpdp@pdp.gov.my

BUTIRAN PELANGGARAN DATA	
1.	**Ringkasan insiden:** **a) Sifat pelanggaran (cth kehilangan, kebocoran, akses tanpa kebenaran, serangan siber, kecacatan teknologi, niat jenayah, kehilangan peralatan dll.)** **b) Bila, di mana dan bagaimana pelanggaran itu berlaku? Adakah kompromi berlaku pada pangkalan data sahaja atau termasuk juga pelanggaran API?** **c) Bilakah pelanggaran itu disedari?** **d) Siapakah dan bagaimana pelanggaran itu disedari?** **e) Berapa lamakah tempoh pelanggaran data itu berlaku?** **f) Apakah punca pelanggaran itu?** **g) Apakah sistem yang terjejas?** **h) Siapakah yang membangunkan sistem yang terjejas? Adakah ia dibangunkan secara dalaman oleh syarikat atau pihak ketiga? Jika ia ialah penyumberan luar, siapakah pembangunnya?** **i) Apakah kategori data organisasi yang dimiliki oleh entiti penyumberan luar? Adakah entiti penyumberan luar mempunyai akses terus kepada rangkaian organisasi?** **j) Bahagian manakah dalam sistem yang dikompromi? Sistem folder fail (NAS / SAN / Storan Awan) atau melibatkan pangkalan data dan sistem aplikasi?** **k) Adakah organisasi anda menggunakan infrastruktur di premis atau infrastruktur awan?** **l) Siapakah pembekal perkhidmatan awan sebelum ini sebelum insiden pelanggaran data? Apakah langkah keselamatan yang tidak mencukupi di pihak pembekal perkhidmatan awan tersebut?**

2.	**Data yang dikompromi:** **a) Jumlah dan jenis data yang telah terjejas (data kewangan, pekerjaan, kesihatan dll.)** **b) Anggaran bilangan subjek data yang terjejas.** **c) Apakah data yang dikumpul, diproses dan disimpan oleh organisasi? Di manakah data tersebut disimpan, dan apakah langkah-langkah keselamatan yang diambil untuk melindungi data tersebut?** **d) Siapa yang mempunyai akses kepada data tersebut, dan bagaimanakah akses tersebut diberikan dan dipantau? Adakah terdapat pihak ketiga yang terlibat dalam pemprosesan data, dan bagaimanakah akses dan penggunaan data mereka dipantau?** **e) Berapa lama data tersebut disimpan, dan bagaimanakah ia dilupuskan?** **f) Adakah organisasi mendapat persetujuan daripada individu untuk memproses data peribadi mereka?** **g) Adakah pelanggaran ini hanya melibatkan warganegara Malaysia? Jika tidak, sila nyatakan negara-negara yang terjejas dan bilangan subjek data yang terjejas.** **h) Adakah organisasi telah menjalankan penilaian impak perlindungan data untuk aktiviti pemprosesan berisiko tinggi?**
3.	**Apakah kemungkinan kemudaratan yang disebabkan oleh kejadian ini? Ia mungkin termasuk:** **a) Ancaman kepada keselamatan diri (Ya/Tidak);** **b) Kecurian identiti (Ya/Tidak);** **c) Kerugian kewangan (Ya/Tidak);** **d) Kerosakan reputasi, penghinaan dan rasa malu (Ya/Tidak);** **e) Kehilangan peluang perniagaan dan pekerjaan (Ya/Tidak);** **f) Lain-lain (sila nyatakan):**

4.	**Langkah-langkah/kawalan keselamatan semasa di organisasi (sebelum kejadian ini):** **a) Sila nyatakan langkah-langkah/kawalan keselamatan semasa di organisasi anda (sebelum kejadian ini).** **b) Adakah organisasi anda diperakui dalam mematuhi:** **- ISO/IEC27002:2022 Keselamatan Maklumat, Keselamatan Siber, dan Perlindungan Privasi (Kawalan Keselamatan Maklumat)** **- ISO/IEC27001:2022 Keselamatan Maklumat, Keselamatan Siber, dan Perlindungan Privasi (Sistem Pengurusan Keselamatan Maklumat)** **- ISO/IEC27701:2019 Teknik Keselamatan (Sistem Pengurusan Maklumat Privasi)** **Jika organisasi anda masih belum diperakui dalam mematuhi Piawaian di atas, sila nyatakan dan terangkan dengan terperinci langkah-langkah & jangka masa untuk diperakui.** **c) Sebarang pematuhan keselamatan data & sistem lain yang organisasi anda telah diperakui dan mematuhinya? (Contoh: PCI DSS)** **d) Adakah sistem organisasi anda melaksanakan penyelarasan Protokol Masa Rangkaian antara semua pelayan & peralatan rangkaian termasuk penyelarasan masa untuk sistem & peralatan keselamatan?** **e) Adakah organisasi mempunyai pelan tindak balas insiden untuk insiden keselamatan siber?** **f) Adakah organisasi telah menjalankan penilaian kelemahan sistem dan infrastrukturnya?** **g) Adakah organisasi mempunyai langkah-langkah yang sesuai untuk melindungi daripada perisian hasad, serangan memancing data dan ancaman keselamatan siber lazim yang lain?** **h) Adakah pekerja kerap dilatih tentang amalan terbaik keselamatan siber?** **i) Adakah pihak ketiga tertakluk kepada kawalan keselamatan siber dan terma kontrak yang sesuai?**
PEMBENDUNGAN DAN PEMULIHAN	
5.	**a) Tindakan yang diambil untuk membendung pelanggaran (cth: Prosedur/arahan yang disediakan untuk meminimumkan risiko kepada keselamatan data)** **b) Tindakan yang diambil untuk memulihkan sebarang data yang hilang dan meminimumkan kerosakan akibat pelanggaran (cth: Pemulihan data melalui pelayan sandaran/pita/cakera optik)**
KOMUNIKASI & NOTIFIKASI	

6.	**a) Pernahkah anda cuba berkomunikasi / berunding secara langsung dengan Aktor Ancaman? (Ya/Tidak);** **b) Pernahkah anda cuba berkomunikasi / berunding dengan Aktor Ancaman melalui ejen / proksinya? (Ya/Tidak);** **c) Adakah anda telah melantik mana-mana ejen / proksi untuk cuba berkomunikasi / berunding secara langsung dengan Aktor Ancaman? (Ya/Tidak);** **d) Adakah anda telah melantik mana-mana ejen / proksi untuk cuba berkomunikasi / berunding dengan Aktor Ancaman melalui ejen / proksinya? (Ya/Tidak).** **Sila sediakan semua bukti berkaitan termasuk transkrip komunikasi suara dengan Aktor Ancaman atau ejen/proksinya.**
7.	**Adakah anda telah memaklumkan pihak-pihak berikut? Apakah kaedah yang digunakan untuk memberitahu?** **a) Badan pengawal selia dan agensi penguatkuasaan undang-undang** **b) Subjek data** **c) Pihak lain yang terjejas** **d) Pemproses data** **e) Pihak berkuasa perlindungan data (luar negara) lain (jika perlu)**