KEMENTERIAN DIGITAL

PESURUHJAYA PERLINDUNGAN DATA PERIBADI MALAYSIA

GARIS PANDUAN PERLINDUNGAN DATA PERIBADI

DBN

PEMBERITAHUAN PELANGGARAN DATA

Versi 1.0

Tarikh Terbitan: 25 Februari 2025

Pesuruhjaya Perlindungan Data Peribadi Malaysia

Hak Cipta Terpelihara

(Pesuruhjaya Perlindungan Data Peribadi Malaysia, 2025)

Tiada mana-mana bahagian penerbitan ini boleh dihasilkan semula, disimpan dalam sistem simpanan kekal, atau dipindahkan dalam sistem simpanan kekal, atau dipindahkan dalam sebarang bentuk atau sebarang cara elektronik, mekanik, penggambaran semula, rakaman dan sebagainya tanpa terlebih dahulu mendapat keizinan daripada pihak Pesuruhjaya Perlindungan Data Peribadi Malaysia.

Alamat:

PESURUHJAYA PERLINDUNGAN DATA PERIBADI MALAYSIA

Aras 8, Galeria PjH, Jalan P4W, Persiaran Perdana

Presint 4, Pusat Pentadbiran Kerajaan Persekutuan

62100 Putrajaya, Malaysia

ISI KANDUNGAN

BIL.	PERKARA	MUKA SURAT
BAHAGIAN A: PENGENALAN		**3**
1.	Latar Belakang	**3**
2.	Peruntukan Undang-Undang	**3**
3.	Tafsiran	**4**
BAHAGIAN B: KEPERLUAN PEMBERITAHUAN PELANGGARAN DATA PERIBADI KEPADA PESURUHJAYA		**4**
4.	Apakah “Pelanggaran Data Peribadi”?	**4**
5.	Pelanggaran Data Peribadi yang Perlu Diberitahu kepada Pesuruhjaya	**6**
6.	Tempoh Masa untuk Pemberitahuan kepada Pesuruhjaya	**8**
7.	Proses Pemberitahuan kepada Pesuruhjaya	**10**
BAHAGIAN C: KEPERLUAN UNTUK PEMBERITAHUAN PELANGGARAN DATA PERIBADI / KOMUNIKASI KEPADA SUBJEK DATA		**13**
8.	Pelanggaran Data Peribadi yang Perlu Diberitahu kepada Subjek Data yang Terjejas	**13**
9.	Tempoh Masa untuk Pemberitahuan kepada Subjek Data	**15**
10.	Cara Pemberitahuan kepada Subjek Data yang Terjejas	**15**
11.	Keperluan Tadbir Urus	**18**
12.	Pelanggaran Data Peribadi melibatkan Pemproses Data	**19**
13.	Kewajipan untuk Menjalankan Penilaian Pelanggaran Data	**19**
14.	Obligasi untuk Menyimpan Rekod Pelanggaran Data Peribadi	**21**
BAHAGIAN D: OBLIGASI PEMBERITAHUAN DI BAWAH UNDANG UNDANG LAIN		**22**
15.	Kewajipan untuk Mematuhi Obligasi Pemberitahuan Lain yang Berkenaan di bawah Undang-undang Malaysia	**22**
16.	Keperluan Pemberitahuan di bawah Undang-undang Malaysia yang Lain	**22**
LAMPIRAN A: CARTA ALIR GAMBARAN KESELURUHAN KEPERLUAN PEMBERITAHUAN PELANGGARAN DATA DI BAWAH AKTA 709		**24**
LAMPIRAN B: BORANG PEMBERITAHUAN PELANGGARAN DATA		**25**

BAHAGIAN A : PENGENALAN

1 Latar Belakang

1.1 Seksyen 12B Akta Perlindungan Data Peribadi 2010 [*Akta 709*] ("**Akta 709**") memperuntukkan obligasi kepada pengawal data untuk memberitahu Pesuruhjaya Perlindungan Data Peribadi ("**Pesuruhjaya**") dan subjek data yang terjejas sekiranya pengawal data mempunyai sebab untuk mempercayai bahawa pelanggaran data peribadi telah berlaku.

1.2 Garis panduan ini menjelaskan tatacara pemberitahuan pelanggaran data peribadi oleh pengawal data kepada Pesuruhjaya dan subjek data yang terjejas bagi memastikan pelanggaran tersebut dikendalikan dengan berkesan serta selaras dengan keperluan Akta 709.

1.3 Contoh-contoh yang diberikan dalam Garis Panduan ini bukanlah bersifat menyeluruh dan hanya disertakan untuk konteks serta tujuan ilustrasi.

1.4 Garis Panduan ini hendaklah dibaca bersama dengan Akta 709, Pekeliling Pesuruhjaya Perlindungan Data Peribadi Bilangan 2 Tahun 2025 (Pemberitahuan Pelanggaran Data) ("**Pekeliling Bil. 2/2025**") dan mana-mana instrumen undang-undang yang dikeluarkan di bawah Akta 709. Garis Panduan ini tidak mengatasi mana-mana undang-undang atau peraturan-peraturan perlindungan data khusus lain yang berkuat kuasa.

2 Peruntukan Undang-Undang

2.1 Garis Panduan yang dibangunkan oleh Pesuruhjaya adalah selaras dengan fungsi Pesuruhjaya di bawah subseksyen 48(g) Akta 709.

2.2 Menurut subseksyen 12B(3) Akta 709, mana-mana pengawal data yang gagal mematuhi subseksyen 12B(1) Akta 709, apabila disabitkan, boleh didenda tidak melebihi dua ratus lima puluh ribu ringgit (RM250,000) atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya.

3 Tafsiran

3.1 Melainkan jika ditakrifkan sebaliknya dalam Garis Panduan ini, istilah-istilah dan pernyataan-pernyataan yang digunakan di sini hendaklah mempunyai makna yang sama seperti yang diberikan di bawah Akta 709, Pekeliling Bil. 2/2025 dan mana-mana instrumen perundangan lain yang berkaitan di bawah Akta 709.

3.2 Dalam Garis Panduan ini, melainkan jika konteksnya menghendaki maksud yang lain:

"insiden keselamatan"	ertinya suatu peristiwa atau kejadian yang menjejaskan atau cenderung untuk menjejaskan perlindungan data atau boleh menjejaskan ketersediaan, kerahsiaan atau integriti data;
"**pelanggaran data peribadi**"	ertinya seperti yang ditakrifkan di bawah seksyen 4 Akta 709 dan tidak terhad kepada pengubahan, penyalinan, pengubahsuaian atau pemusnahan.

BAHAGIAN B: KEPERLUAN PEMBERITAHUAN PELANGGARAN DATA PERIBADI KEPADA PESURUHJAYA

4 Apakah "Pelanggaran Data Peribadi"?

4.1 Obligasi pemberitahuan di bawah Akta 709 hanya terpakai sekiranya berlaku "pelanggaran data peribadi" seperti yang ditakrifkan oleh Akta 709 dan Pekeliling Bil. 2/2025. Oleh itu, adalah penting bagi pengawal data untuk mengenalpasti dan menentukan apakah yang dimaksudkan dengan "pelanggaran data peribadi".

4.2 Suatu "pelanggaran data peribadi" secara umum merujuk kepada apa-apa kejadian / insiden yang menyebabkan atau berkemungkinan menyebabkan pelanggaran, kehilangan, salah guna atau akses tanpa kebenaran ke atas data

peribadi. Suatu pelanggaran data peribadi mungkin disebabkan oleh tindakan tidak sengaja atau sengaja, sama ada oleh pelaku ancaman dalaman atau luaran.

Contoh:

(i) Akses kepada data peribadi yang dipegang pengawal data oleh pihak ketiga tanpa kebenaran.

(ii) Seorang pekerja secara tidak sengaja menghantar e-mel yang mengandungi data peribadi kepada penerima yang salah.

(iii) Seorang pekerja secara tidak sengaja kehilangan / tersalah letak komputer riba milik syarikat yang mengandungi data peribadi yang tidak disulitkan, menyebabkan potensi akses tanpa kebenaran ke atas data peribadi.

(iv) Seorang pekerja yang mempunyai akses yang dibenarkan kepada data peribadi sensitif dengan sengaja mencuri data peribadi (contohnya maklumat pelanggan) dan menjualnya kepada pihak ketiga.

(v) Pihak luar memperoleh akses secara tidak sah kepada rangkaian atau akaun pengguna pengawal data dan mengekstrak data peribadi.

(vi) Konfigurasi sistem yang salah menyebabkan kehilangan data peribadi atau perkongsian data peribadi yang tidak disengajakan dengan pihak ketiga.

(vii) Pengubahan data peribadi tanpa kebenaran.

(viii) Kehilangan sementara atau kekal data peribadi (seperti situasi di mana pihak ketiga tanpa kebenaran menahan data peribadi sebagai tebusan dengan menghalang pengawal data daripada memperoleh akses kepadanya, atau situasi di mana kunci penyahsulitan sepadan untuk data yang disulitkan telah hilang).

(ix) Seorang pekerja tersalah letak atau menghilangkan dokumen fizikal yang mengandungi data peribadi seperti rekod perubatan, penyata kewangan dan sebagainya semasa transit atau penyimpanan.

(x) Seorang pekerja meninggalkan maklumat data peribadi seperti borang yang mengandungi butiran pengenalan tanpa pengawasan di atas meja atau di ruangan awam di mana individu lain boleh melihatnya tanpa kebenaran.

(xi) Penghantaran surat atau borang yang mengandungi data peribadi seperti invois atau penyata kewangan kepada penerima yang salah.

5 Pelanggaran Data Peribadi yang Perlu Diberitahu kepada Pesuruhjaya

5.1 Bukan semua pelanggaran data peribadi perlu diberitahu kepada Pesuruhjaya. Pengawal data hanya perlu memberitahu Pesuruhjaya mengenai pelanggaran data peribadi sekiranya pelanggaran data peribadi tersebut mengakibatkan atau bermungkinan mengakibatkan "*kemudaratan yang ketara*".

Apakah "kemudaratan yang ketara"?

5.2 Pelanggaran data peribadi dianggap sebagai mengakibatkan atau berkemungkinan mengakibatkan "*kemudaratan yang ketara*" jika terdapat risiko bahawa data peribadi yang terjejas:

5.2.1 boleh mengakibatkan kecederaan fizikal, kerugian kewangan, kesan negatif terhadap rekod kredit, kerosakan atau kehilangan harta benda;

5.2.2 boleh disalah guna untuk tujuan yang menyalahi undang-undang;

5.2.3 mengandungi data peribadi sensitif;

5.2.4 mengandungi data peribadi dan maklumat peribadi yang apabila digabungkan berpotensi untuk membolehkan penipuan identiti; atau

5.2.5 berskala signifikan.

Apakah "berskala signifikan"?

5.3 Pelanggaran data peribadi dianggap "*berskala signifikan*" jika bilangan subjek data yang terjejas melebihi satu ribu (1,000).

Contoh Pelanggaran Data Peribadi:

5.4 Contoh-contoh senario pelanggaran data peribadi yang mana pengawal data hendaklah memberitahu Pesuruhjaya:

Contoh	**Sama ada Pemberitahuan kepada Pesuruhjaya Perlu**
Seorang pekerja kehilangan komputer riba yang mengandungi data peribadi para pelanggan.	Ya, sekiranya jenis set data yang terjejas berkemungkinan menyebabkan "*kemudaratan yang ketara*" atau jika pelanggaran tersebut melebihi 1,000 subjek data.
Pihak ketiga tanpa kebenaran memperoleh akses kepada rekod perubatan para pesakit.	Ya, sebab pelanggaran yang melibatkan "*data peribadi sensitif*" (iaitu rekod perubatan) dianggap sebagai "*kemudaratan yang ketara*" tanpa mengira sama ada jumlah subjek data yang terjejas melebihi 1,000 subjek data.
Kecurian komputer riba yang disulitkan yang mengandungi	Tidak, penzahiran alamat e-mel para pekerja tidak berkemungkinan

Contoh	**Sama ada Pemberitahuan kepada Pesuruhjaya Perlu**
alamat e-mel seramai 200 pekerja dalam sebuah organisasi.	menyebabkan sebarang "*kemudaratan yang ketara*".
Rekod perubatan di sebuah hospital tidak dapat diakses untuk sementara akibat serangan siber.	Ya, sebab pelanggaran yang melibatkan "*data peribadi sensitif*" (iaitu, rekod perubatan) dianggap berpotensi menyebabkan "*kemudaratan yang ketara"* tanpa mengambil kira sama ada jumlah subjek data yang terjejas melebihi 1,000.
Suatu e-mel yang mengandungi penyata akaun pelanggan dihantar kepada penerima yang salah.	Ya, sebab data peribadi yang terjejas melibatkan maklumat kewangan subjek data.

5.5 Pengawal data hendaklah menilai sama ada "pelanggaran data peribadi" memenuhi salah satu kriteria pemberitahuan yang disenaraikan dalam perenggan 5.2 di atas. Jika ya, pengawal data hendaklah memberitahu pelanggaran data peribadi kepada Pesuruhjaya.

6 Tempoh Masa untuk Pemberitahuan kepada Pesuruhjaya

6.1 Pemberitahuan hendaklah dibuat dengan secepat yang dapat dilaksanakan dalam tempoh tujuh puluh dua (72) jam selepas berlakunya pelanggaran data peribadi tersebut.

Pengiraan Tempoh Masa 72 Jam untuk Pemberitahuan

6.2 Setelah pengawal data dimaklumkan oleh individu, organisasi media atau mana-mana sumber lain, atau apabila pengawal data sendiri mengesan insiden keselamatan, pengawal data hendaklah menjalankan penyiasatan awal bagi memastikan sama ada pelanggaran data peribadi benar-benar telah berlaku.

Contoh:

Berikut adalah contoh pengiraan tempoh 72 jam untuk membuat pemberitahuan pelanggaran data kepada Pesuruhjaya:

(i) Apabila kunci USB yang mengandungi data peribadi tidak disulitkan dilaporkan hilang, tempoh 72 jam untuk pemberitahuan kepada Pesuruhjaya bermula sebaik sahaja kehilangan tersebut dimaklumkan kepada pengawal data.

(ii) Tempoh 72 jam untuk pemberitahuan kepada Pesuruhjaya bermula sebaik sahaja pengawal data secara tidak sengaja menghantar data peribadi tanpa kebenaran dan menyedari kesilapannya.

(iii) Dalam kes yang berkemungkinan melibatkan pencerobohan atau penyusupan ke dalam rangkaian pengawal data, tempoh 72 jam untuk pemberitahuan kepada Pesuruhjaya bermula sebaik sahaja pengawal data semasa memeriksa sistemnya, mengesahkan bahawa sistem tersebut sebenarnya telah terjejas.

(iv) Serangan perisian tebusan *(ransomware)* ialah sejenis serangan siber di mana penjenayah menyulitkan data mangsa dan menghalang mereka daripada mengakses sistem mereka. Penjenayah kemudian menuntut bayaran tebusan untuk memulihkan akses mangsa. Dalam kes sedemikian, tempoh 72 jam untuk pemberitahuan kepada Pesuruhjaya bermula apabila pengawal data menyedari bahawa mereka telah kehilangan akses kepada data mereka atau, setelah dimaklumkan oleh penjenayah siber mengenai penggodaman, mereka menjalankan

penilaian sendiri dan mengesahkan bahawa pelanggaran data peribadi telah berlaku.

(v) Sekiranya pemproses data memproses data bagi pihak pengawal data, tempoh 72 jam untuk pemberitahuan kepada Pesuruhjaya bermula sebaik sahaja pemproses data memaklumkan pengawal data mengenai pelanggaran data peribadi atau apabila pengawal data sendiri memperoleh bukti jelas bahawa pelanggaran data peribadi telah berlaku, mengikut mana-mana yang terdahulu.

7 Proses Pemberitahuan kepada Pesuruhjaya

Format dan Saluran Pemberitahuan

7.1 Pemberitahuan kepada Pesuruhjaya hendaklah dibuat melalui salah satu saluran berikut:

7.1.1 melengkapkan borang pemberitahuan yang tersedia di laman sesawang rasmi Jabatan Perlindungan Data Peribadi (JPDP) di www.pdp.gov.my;

7.1.2 melengkapkan borang pemberitahuan dalam **Lampiran B** dan menghantarnya ke alamat e-mel rasmi di dbnpdp@pdp.gov.my; atau

7.1.3 melengkapkan borang pemberitahuan dalam **Lampiran B** dan menghantarnya dalam bentuk salinan keras kepada Pesuruhjaya.

Pemberitahuan secara berperingkat

7.2 Pengawal data hendaklah memastikan bahawa semua maklumat yang diperlukan / mandatori dalam borang pemberitahuan yang dinyatakan dalam perenggan 7.1 dilengkapkan. Pemberitahuan kepada Pesuruhjaya melalui

kaedah yang dinyatakan dalam perenggan 7.1 hendaklah dikemukakan dalam tempoh tujuh puluh dua (72) jam dari masa yang ditetapkan.

7.3 Pesuruhjaya akan mengeluarkan notis pengesahan kepada pengawal data setelah menerima pemberitahuan pelanggaran data peribadi tersebut. Pemberitahuan tersebut dianggap tidak diterima Pesuruhjaya tanpa notis pengesahan sedemikian.

7.4 Sebagai tambahan kepada ruang yang diperlukan / mandatori dalam borang pemberitahuan yang dikemukakan di bawah perenggan 7.1, pengawal data juga hendaklah memberikan Pesuruhjaya maklumat seperti yang berikut:

7.4.1 Butiran pelanggaran data peribadi yang telah berlaku termasuk:

7.4.1.1 tarikh dan masa pelanggaran data peribadi disedari oleh pengawal data;

7.4.1.2 jenis data peribadi dan pelanggaran data peribadi;

7.4.1.3 kaedah mengenal pasti pelanggaran data peribadi yang dipercayai sebagai punca pelanggaran data peribadi;

7.4.1.4 jumlah subjek data yang terjejas;

7.4.1.5 anggaran rekod data yang terjejas; dan

7.4.1.6 sistem data peribadi yang terjejas yang menyebabkan pelanggaran tersebut berlaku;

7.4.2 kemungkinan yang berlaku akibat daripada pelanggaran data;

7.4.3 kronologi insiden yang menyebabkan kehilangan kawalan ke atas data peribadi;

7.4.4 langkah-langkah yang diambil atau dicadang untuk diambil oleh pengawal data bagi menangani pelanggaran data peribadi tersebut

termasuk langkah-langkah yang diambil atau akan di ambil untuk mengurangkan kemungkinan kesan buruk pelanggaran data peribadi;

7.4.5 langkah-langkah yang diambil atau dicadang untuk diambil untuk menangani subjek data yang terjejas; dan

7.4.6 butiran pegawai perlindungan data atau maklumat perhubungan lain daripadanya tentang pelanggaran data peribadi boleh diperolehi.

7.5 Setakat mana yang tidak mungkin bagi pengawal data untuk menyediakan semua maklumat yang diminta dalam perenggan 7.4 semasa pemberitahuan awal kepada Pesuruhjaya, maklumat tersebut boleh diberikan secara berperingkat, secepat yang dapat dilaksanakan dan tidak lewat daripada tiga puluh (30) hari dari tarikh pemberitahuan yang dibuat dalam perenggan 7.1.

Pelanggaran Data Peribadi yang Melibatkan Berbilang Pengawal Data

7.6 Jika pelanggaran data peribadi melibatkan lebih daripada satu (1) pengawal data, setiap pengawal data hendaklah mengemukakan pemberitahuan pelanggaran data yang berasingan kepada Pesuruhjaya.

Kelewatan Pemberitahuan Pelanggaran Data

7.7 Sekiranya pengawal data gagal memberitahu Pesuruhjaya dalam tempoh tujuh puluh dua (72) jam, pengawal data hendaklah menyerahkan notis secara bertulis kepada Pesuruhjaya dengan menyatakan sebab-sebab kelewatan serta mengemukakan bukti yang menyokong alasan tersebut. Bukti tersebut hendaklah merangkumi dokumentasi berkenaan garis masa insiden, komunikasi dalaman dan sebarang isu teknikal atau faktor luaran yang telah menyumbang kepada kelewatan. Semua dokumen berkaitan hendaklah dikemukakan bersama pemberitahuan tersebut.

Pegawai Perhubungan dan Penyediaan Bantuan bagi Penyiasatan oleh Pesuruhjaya

7.8 Sekiranya pengawal data tertakluk kepada keperluan mandatori untuk melantik pegawai perlindungan data di bawah Seksyen 12A Akta 709, pegawai perlindungan data tersebut hendaklah bertindak sebagai pegawai perhubungan bagi sebarang pertanyaan atau permintaan daripada Pesuruhjaya berkaitan pelanggaran data peribadi. Sekiranya pengawal data tidak tertakluk kepada keperluan mandatori untuk melantik pegawai perlindungan data, pengawal data hendaklah menamakan atau menetapkan seorang wakil yang mempunyai kedudukan kanan dan kepakaran yang mencukupi untuk bertindak sebagai pegawai perhubungan.

7.9 Selaras dengan Seksyen 105 Akta709, Pesuruhjaya boleh menjalankan suatu penyiasatan berhubung dengan pengawal data untuk memastikan sama ada perbuatan, amalan atau permintaan itu melanggar peruntukan Akta 709.

7.10 Pesuruhjaya boleh mengarahkan pengawal data untuk mengemukakan rekod berhubung pemberitahuan pelanggaran data atau mana-mana dokumen laporan apabila diminta selaras dengan Seksyen 121 Akta 709.

BAHAGIAN C: KEPERLUAN UNTUK PEMBERITAHUAN PELANGGARAN DATA PERIBADI / KOMUNIKASI KEPADA SUBJEK DATA

8 Pelanggaran Data Peribadi yang Perlu Diberitahu kepada Subjek Data yang Terjejas

8.1 Pengawal data hendaklah memberitahu subjek data mengenai pelanggaran data peribadi yang berlaku sekiranya pelanggaran tersebut mengakibatkan atau berkemungkinan mengakibatkan "*kemudaratan yang ketara*" kepada subjek data.

8.2 Perenggan 5.2 menetapkan tafsiran "*kemudaratan yang ketara*" dalam konteks pemberitahuan kepada Pesuruhjaya, dan tafsiran yang sama juga terpakai dalam menentukan "kemudaratan yang ketara" bagi tujuan pemberitahuan kepada subjek data. Namun begitu, kriteria "*berskala signifikan"* di bawah perenggan 5.3 tidak terpakai dalam menentukan sama ada pemberitahuan kepada subjek data yang terjejas diperlukan.

Contoh Pelanggaran Data Peribadi yang Memerlukan Pemberitahuan kepada Subjek Data yang Terjejas

8.3 Contoh-contoh yang senario pelanggaran data peribadi yang mana pengawal data perlu memberitahu subjek data yang terjejas:

Contoh	**Sama ada Pemberitahuan kepada subjek data Perlu**
Sebuah institusi kewangan mengalami serangan siber yang mengakibatkan kecurian maklumat peribadi dan kewangan pelanggan termasuk nama, nombor akaun dan kata laluan.	Ya, risiko kemudaratan yang ketara adalah tinggi kerana kerugian kewangan mungkin berlaku dan data tersebut termasuk maklumat yang boleh digunakan untuk membolehkan penipuan identiti. Oleh itu, subjek data perlu dimaklumkan mengenai pelanggaran tersebut.
Seorang penjenayah siber menggodam pelayan yang mengandungi data peribadi dan kewangan pelanggan dan memperoleh kawalan ke atas pelayan milik pembekal farmasi. Bagaimanapun, penjenayah siber tidak dapat mengakses data peribadi dan kewangan tersebut	Tidak, dalam situasi ini, subjek data tidak perlu dimaklumkan kerana data dilindungi oleh langkah keselamatan yang menjadikan maklumat itu tidak dapat difahami atau tidak bermakna kepada penjenayah siber. Walau bagaimanapun, pengawal data perlu memaklumkan Pesuruhjaya mengikut cara yang ditetapkan.

Contoh	Sama ada Pemberitahuan kepada subjek data Perlu
kerana pembekal farmasi telah melaksanakan dua lapisan langkah keselamatan.	
Penjenayah siber memintas sistem keselamatan pelayan milik penjual langsung dan memperoleh kawalan keseluruhan data pada pelayan. Penjenayah siber itu mengancam untuk memadamkan data pada pelayan jika syarikat itu tidak membayar wang tebusan. Penjual langsung tidak mempunyai sebarang sandaran data tersebut.	Ya, dalam situasi ini, subjek data perlu dimaklumkan kerana terdapat risiko kehilangan data peribadi dan kewangan subjek data.

9 Tempoh Masa untuk Pemberitahuan kepada Subjek Data

9.1 Pemberitahuan kepada subjek data yang terjejas seperti yang dirujuk dalam perenggan 8.1 hendaklah dibuat tanpa kelengahan yang tidak perlu, tidak lewat daripada tujuh (7) hari selepas pemberitahuan pelanggaran data dibuat kepada Pesuruhjaya di bawah perenggan 7.1.

10 Cara Pemberitahuan kepada Subjek Data yang Terjejas

10.1 Pemberitahuan kepada subjek data yang terjejas hendaklah diberikan secara perseorangan dan terus kepada subjek data dengan cara yang praktikal menggunakan bahasa yang boleh difahami sesuai dengan keadaan untuk membolehkan subjek data mengambil langkah berjaga-jaga yang diperlukan

atau tindakan lain untuk melindungi diri mereka daripada kemungkinan kesan buruk akibat pelanggaran data peribadi tersebut.

Maklumat yang Perlu Diberikan dalam Pemberitahuan

10.2 Pemberitahuan pelanggaran data peribadi oleh pengawal data kepada subjek data yang terjejas hendaklah termasuk maklumat-maklumat berikut:

10.2.1 maklumat mengenai pelanggaran data peribadi yang telah berlaku;

10.2.2 butiran kemungkinan yang berlaku akibat daripada pelanggaran data peribadi;

10.2.3 langkah-langkah yang diambil atau dicadang untuk diambil oleh pengawal data bagi menangani pelanggaran data peribadi, termasuk langkah yang bersesuaian untuk mengurangkan kemungkinan kesan buruk akibat pelanggaran data peribadi;

10.2.4 langkah-langkah yang boleh diambil oleh subjek data yang terjejas untuk menghapus atau mengurang sebarang kemungkinan kesan buruk akibat pelanggaran data; dan

10.2.5 butiran pegawai perlindungan data atau maklumat perhubungan lain, yang daripadanya maklumat lanjut mengenai pelanggaran data peribadi boleh diperolehi.

Kaedah Pemberitahuan

10.3 Sekiranya pemberitahuan secara langsung tidak dapat dilaksanakan atau memerlukan usaha yang tidak seimbang, pengawal data boleh menggunakan kaedah pemberitahuan alternatif seperti komunikasi awam atau mana-mana kaedah serupa yang membolehkan subjek data yang terjejas dimaklumkan mengenai pelanggaran data peribadi dengan berkesan.

10.4 Contoh-contoh "*usaha yang tidak setimpal*" termasuk yang berikut:

10.4.1 pengawal data dikehendaki untuk menghubungi sejumlah besar subjek data di pelbagai negeri atau negara, di mana tindakan tersebut akan mengakibatkan beban logistik, pentadbiran atau kewangan yang berlebihan; atau

10.4.2 pengawal data perlu memberitahu subjek data yang telah memberikan maklumat perhubungan yang tidak dikemaskini atau tidak tepat, di mana tindakan tersebut memerlukan sumber yang besar untuk mendapatkan butiran hubungan yang betul bagi setiap subjek data.

Contoh kaedah untuk memaklumkan subjek data yang terjejas secara perseorangan:

- e-mel;
- SMS;
- mesej langsung; dan
- komunikasi melalui pos.

Contoh komunikasi awam:

- notis pemberitahuan di laman sesawang rasmi;
- notis dalam media cetak;
- siaran media sosial melalui halaman atau akaun rasmi pengawal data; dan
- pemberitahuan automatik *(push notification)*.

10.5 Bentuk pemberitahuan yang digunakan untuk memaklumkan subjek data yang terjejas tentang pelanggaran data peribadi hendaklah dihantar secara berasingan daripada maklumat lain, seperti pengemaskinian secara berkala, surat berita atau mesej standard supaya komunikasi pelanggaran tersebut jelas dan telus.

11 Keperluan Tadbir Urus

11.1 Pengawal data hendaklah menyediakan pelan pengurusan dan respons pelanggaran data yang mencukupi.

11.2 Fokus terhadap pelan pengurusan dan respons pelanggaran hendaklah untuk memastikan pengawal data dapat mengenal pasti pelanggaran data peribadi dengan segera, mengambil langkah yang sewajarnya untuk membendung dan mengurangkan pelanggaran serta memastikan pematuhan mereka terhadap obligasi dalam pemberitahuan pelanggaran data.

11.3 Pelan pengurusan dan respons pelanggaran data peribadi hendaklah sekurang-kurangnya menggariskan dasar dan prosedur untuk menangani perkara-perkara berikut:

11.3.1 prosedur pengenalpastian dan pelaporan pelanggaran data peribadi;

11.3.2 peranan dan tanggungjawab pihak berkepentingan yang berkaitan (contohnya, pelan respons pelanggaran data, pegawai perlindungan data);

11.3.3 langkah-langkah untuk membendung dan mengurangkan impak pelanggaran;

11.3.4 langkah-langkah untuk menentukan sama ada perlu memberitahu Pesuruhjaya dan / atau subjek data yang terjejas;

11.3.5 pelan komunikasi untuk memberitahu Pesuruhjaya dan / atau subjek data yang terjejas; dan

11.3.6 kajian pasca insiden.

11.4 Pengawal data hendaklah juga menjalankan latihan berkala serta latihan kesedaran dan simulasi bagi memastikan pekerja-pekerjanya sedar tentang peranan dan tanggungjawab mereka dalam membantu pengawal data memberi respons kepada pelanggaran data peribadi.

12 Pelanggaran Data Peribadi melibatkan Pemproses Data

12.1 Pemberitahuan pelanggaran data peribadi mandatori di bawah seksyen 12B Akta 709 tidak terpakai kepada pemproses data secara langsung.

12.2 Pengawal data perlu mengenakan obligasi melalui kontrak ke atas pemproses data untuk segera memberitahu mereka tentang pelanggaran data yang telah berlaku dan untuk menyediakan semua bantuan yang munasabah serta perlu kepada pengawal data untuk memenuhi obligasi pengawal data dalam pemberitahuan pelanggaran data di bawah Akta 709.

13 Kewajipan untuk Menjalankan Penilaian Pelanggaran Data

13.1 Pengawal data hendaklah bertindak segera sebaik sahaja menyedari sebarang pelanggaran data peribadi untuk menilai, membendung dan mengurangkan impak yang mungkin disebabkan akibat pelanggaran data tersebut.

13.2 Penyiasatan pelanggaran data boleh mengambil masa yang lama dan pengawal data mungkin tidak dapat memperoleh pemahaman yang lengkap tentang pelanggaran semasa peringkat awal penyiasatan mereka terutamanya jika pelanggaran itu rumit.

13.3 Sebaik sahaja terdapat pemberitahuan mengenai pelanggaran data peribadi kepada pengawal data, mereka hendaklah mempertimbangkan tindakan pembendungan berikut dengan segera, yang mana berkenaan:

13.3.1 asingkan dan putuskan sambungan pangkalan data atau sistem yang terjejas daripada rangkaian;

13.3.2 menyekat atau menyahaktif hak akses yang terjejas;

13.3.3 menghentikan amalan yang dikenal pasti telah menyebabkan pelanggaran data tersebut; dan

13.3.4 menentukan sama ada data yang hilang boleh dipulihkan atau sama ada sebarang tindakan pemulihan segera boleh diambil untuk meminimumkan kemudaratan lanjut yang disebabkan oleh pelanggaran tersebut.

13.4 Semasa siasatan awal suatu pelanggaran data, pengawal data hendaklah mengenalpasti maklumat-maklumat berikut:

13.4.1 jenis data peribadi yang terlibat;

13.4.2 bilangan subjek data yang terjejas;

13.4.3 sistem, pelayan, pangkalan data, platform dan perkhidmatan yang terjejas;

13.4.4 kronologi peristiwa yang menyebabkan pelanggaran data;

13.4.5 tahap keseriusan pelanggaran data;

13.4.6 punca utama pelanggaran data dan sama ada ia masih berterusan;

13.4.7 kemudaratan dan potensi kemudaratan yang mungkin disebabkan akibat pelanggaran data tersebut;

13.4.8 langkah-langkah yang wajar diambil untuk membendung pelanggaran data dan mengurangkan kemungkinan kesan buruknya; dan

13.4.9 tindakan-tindakan pemulihan yang wajar diambil untuk mengurangkan kemudaratan kepada subjek data yang terjejas.

13.5 Maklumat di atas juga boleh membantu pengawal data dalam menentukan sama ada bantuan luaran (contohnya, pakar perlindungan data atau pakar forensik teknikal) diperlukan untuk membantu mereka memberi respons dan membendung pelanggaran data peribadi tersebut.

13.6 Pengawal data hendaklah menjalankan penilaian pasca pelanggaran untuk mengkaji keberkesanan pelan pengurusan dan respons pelanggaran data serta amalan dan dasar perlindungan data untuk mencegah insiden yang serupa daripada berulang.

14 Obligasi untuk Menyimpan Rekod Pelanggaran Data Peribadi

14.1 Pengawal data hendaklah menyimpan rekod dan menyenggara daftar yang memperincikan pelanggaran data peribadi untuk tempoh sekurang-kurangnya dua (2) tahun dari tarikh pemberitahuan pelanggaran data peribadi kepada Pesuruhjaya termasuk pelanggaran yang tidak memenuhi kriteria pemberitahuan kepada Pesuruhjaya dan/atau subjek data yang terjejas. Daftar tersebut hendaklah sekurang-kurangnya mendokumentasikan maklumat-maklumat berikut:

14.1.1 perihalan pelanggaran data peribadi termasuk tarikh dan masa pengawal data menyedari pelanggaran data peribadi, analisis dan pengenalpastian punca utama, jenis data peribadi yang terlibat, anggaran jumlah subjek data yang terjejas, anggaran jumlah rekod data yang terjejas dan sistem data peribadi yang terjejas yang membenarkan pelanggaran itu berlaku;

14.1.2 perihalan kemungkinan yang berlaku akibat daripada pelanggaran data peribadi tersebut;

14.1.3 deskripsi kronologi peristiwa yang menyebabkan pelanggaran data peribadi;

14.1.4 langkah-langkah pembendungan dan pemulihan yang diambil untuk menangani pelanggaran data peribadi tersebut; dan

14.1.5 butiran pemberitahuan yang dibuat kepada Pesuruhjaya dan/atau subjek data yang terjejas serta justifikasi untuk tidak membuat pemberitahuan, yang mana berkenaan.

14.2 Pengawal data bebas menentukan kaedah dan format untuk digunakan semasa mendokumentasikan pelanggaran dengan syarat dokumentasi tersebut jelas, ringkas dan membolehkan Pesuruhjaya mengesahkan bahawa pengawal data telah mematuhi kehendak dokumentasi di atas.

14.3 Dokumentasi pelanggaran data peribadi dalam perenggan 14.1 di atas hendaklah tersedia apabila diminta oleh Pesuruhjaya.

BAHAGIAN D: OBLIGASI PEMBERITAHUAN DI BAWAH UNDANG-UNDANG LAIN

15 Kewajipan untuk Mematuhi Obligasi Pemberitahuan Lain yang Berkenaan di bawah Undang-undang Malaysia

15.1 Obligasi pemberitahuan pelanggaran data peribadi secara mandatori di bawah Akta 709 terpakai secara berasingan dan serentak dengan mana-mana obligasi pemberitahuan lain serupa yang mungkin terpakai kepada pengawal data di bawah undang-undang dan peraturan-peraturan sedia ada di Malaysia.

15.2 Pengawal data hendaklah mengenal pasti keperluan pemberitahuan yang berkaitan dan mungkin terpakai kepada mereka serta mewujudkan proses serta prosedur dalaman bagi memudahkan pematuhan terhadap pelbagai keperluan pemberitahuan yang berkenaan.

16 Keperluan Pemberitahuan di bawah Undang-undang Malaysia yang Lain

16.1 Di bawah adalah senarai yang tidak muktamad mengenai keperluan pemberitahuan yang dikenakan di bawah undang-undang dan peraturan-peraturan Malaysia yang mungkin terpakai kepada pengawal data:

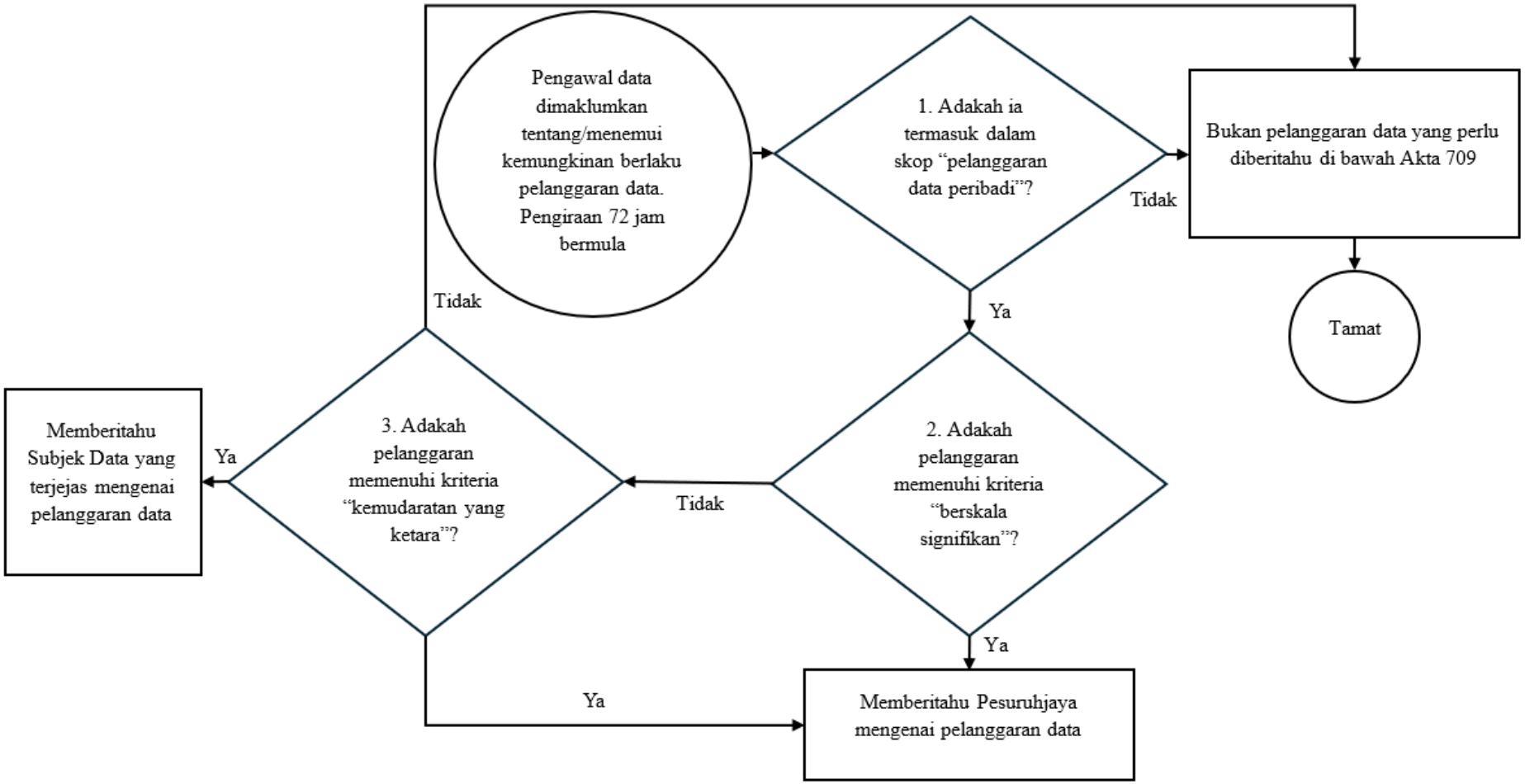
16.1.1 pemberitahuan kepada Polis Diraja Malaysia ("**PDRM**") yang mana pelanggaran data melibatkan aktiviti jenayah;

16.1.2 pemberitahuan kepada pengawal selia sektor seperti Bank Negara Malaysia ("**BNM**"), Suruhanjaya Sekuriti Malaysia ("**SC**") serta Suruhanjaya Komunikasi dan Multimedia Malaysia ("**SKMM**") menurut keperluan-keperluan pemberitahuan insiden siber atau pelanggaran data sektor; dan

16.1.3 pemberitahuan kepada Ketua Eksekutif Agensi Keselamatan Siber Negara ("**NACSA**") dan Ketua-Ketua Sektor Infrastruktur Maklumat Kritikal Negara ("**NCII**") ("**Ketua-Ketua Sektor NCII**"), di mana pengawal data ialah Entiti NCII yang ditetapkan di bawah Akta Keselamatan Siber 2024.

16.2 Sila ambil perhatian bahawa senarai di atas untuk tujuan rujukan sahaja. Pengawal data hendaklah menjalankan penilaian mereka sendiri untuk mengenal pasti keperluan pemberitahuan di bawah undang-undang dan peraturan-peraturan lain di Malaysia yang terpakai.

LAMPIRAN A: CARTA ALIR GAMBARAN KESELURUHAN KEPERLUAN PEMBERITAHUAN PELANGGARAN DATA DI BAWAH AKTA 709



LAMPIRAN B: BORANG PEMBERITAHUAN PELANGGARAN DATA

PEMBERITAHUAN PELANGGARAN DATA

Borang pemberitahuan ini digunakan apabila pengawal data ingin melaporkan pelanggaran data kepada Pesuruhjaya Perlindungan Data Peribadi ("**Pesuruhjaya**").

Sila ambil perhatian bahawa maklumat yang diminta dalam borang pemberitahuan ini tidak muktamad. Pesuruhjaya mungkin menghendaki butiran lanjut mengenai insiden untuk memudahkan siasatan.

Di mana dan setakat mana tidak dapat memberikan semua maklumat yang diminta dalam borang pemberitahuan, adalah memadai untuk melengkapkan borang ini setakat mana maklumat yang ada. Maklumat tambahan hendaklah diberikan kepada Pesuruhjaya secara berperingkat secepat mungkin tidak lewat daripada tiga puluh (30) hari dari tarikh pemberitahuan awal.

BUTIRAN PENGAWAL DATA

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

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

Individu untuk dihubungi

Nama : ----------

Jawatan : ----------

Nombor Telefon : ----------

E-mel : ----------

Tarikh : ----------

Tandatangan : ----------

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

Penyerahan pemberitahuan:

PESURUHJAYA PERLINDUNGAN DATA PERIBADI
Tingkat 8, Galeria PjH, Jalan P4W
Persiaran Perdana, Presint 4
62100 W.P Putrajaya
atau melalui e-mel: dbnpdp@pdp.gov.my

SEKSYEN A: MAKLUMAT ASAS

1. Adakah ini merupakan pemberitahuan baharu atau kemaskini kepada pemberitahuan terdahulu yang dikemukakan kepada Pesuruhjaya?

☐ Pemberitahuan baharu

☐ Kemaskini. Sila nyatakan nombor rujukan pemberitahuan asal:

2. Jika ini merupakan pemberitahuan baharu, adakah anda mengemukakan pemberitahuan ini dalam masa 72 jam selepas menyedari pelanggaran data peribadi tersebut?

☐ Ya

☐ Tidak. Sila nyatakan sebab-sebab kelewatan beserta bukti sokongan :

SEKSYEN B: BUTIRAN PELANGGARAN DATA PERIBADI

3. Bilakah organisasi anda menyedari tentang pelanggaran data peribadi?

(Sila sertakan tarikh dan masa apabila organisasi anda menyedari pelanggaran tersebut)

Tarikh :	*Masa:*

4. Bagaimanakah organisasi anda menyedari pelanggaran data peribadi?

(Sila berikan penerangan ringkas mengenai cara organisasi anda mengesan pelanggaran data peribadi tersebut)

5. Bagaimanakah data peribadi terjejas atau dikompromi?

(Tandakan semua jawapan yang berkenaan)

☐ Data telah dizahir kepada pihak yang tidak diingini

☐ Data telah hilang

☐ Data tidak ada buat sementara waktu

☐ Data telah dikeluarkan / dicuri

☐ Akses kepada data peribadi tanpa kebenaran

☐ Lain-lain:

6. Apakah punca sebenar atau punca yang disyaki bagi insiden ini?

(Pilih satu sahaja)

☐ Insiden siber

☐ Kesilapan manusia

☐ Kesilapan sistem

☐ Kecurian / penyalahgunaan maklumat oleh pelaku berniat jahat

☐ Lain-lain:

7. Bagaimanakah punca sebenar insiden di atas dikenal pasti? (Sila nyatakan)

8. Apakah sistem atau aplikasi yang terjejas dalam insiden pelanggaran data peribadi ini? (Sila nyatakan)

9. Di manakah lokasi penyimpanan data peribadi yang terjejas akibat pelanggaran data peribadi ini?

☐ Malaysia

☐ Negara lain (Sila nyatakan)

10. Apakah insiden pelanggaran data peribadi ini?

☐ Dalam tindakan

☐ Telah diperbetulkan / dibendung

11. Adakah terdapat mana-mana pihak lain yang terjejas oleh pelanggaran data peribadi ini (contohnya, pengawal data atau pemproses data lain)?

☐ Tidak.

☐ Ya. Sila senaraikan pihak-pihak ini:

SEKSYEN C: BUTIRAN DATA YANG DIKOMPROMI

12. Apakah jenis data peribadi yang terjejas?

13. Berapakah jumlah subjek data yang terjejas atau berkemungkinan terjejas?

14. Adakah pelanggaran data peribadi ini hanya menjejaskan subjek data yang merupakan warganegara Malaysia?

☐ Ya.

☐ Tidak. Pelanggaran ini juga menjejaskan subjek data dalam bidang kuasa negara berikut:

15. Apakah kemudaratan atau risiko yang berkemungkinan timbul akibat pelanggaran data peribadi terhadap subjek data?

(Tandakan semua jawapan yang berkenaan)

☐ Kemudaratan fizikal atau ancaman terhadap keselamatan

☐ Kerugian kewangan

☐ Pencurian atau penipuan identiti

☐ Data digunakan untuk tujuan yang menyalahi undang-undang

☐ Data mengandungi data peribadi sensitif

☐ Data mengandungi maklumat kewangan

☐ Tiada potensi kemudaratan kepada subjek data

☐ Lain-lain (Sila nyatakan)

SEKSYEN D: TINDAKAN PEMBENDUNGAN DAN PEMULIHAN

16. Apakah tindakan yang telah atau akan diambil untuk membendung dan mengurangkan kemudaratan atau risiko yang mungkin timbul akibat pelanggaran data peribadi tersebut?

17. Apakah tindakan yang telah atau akan diambil untuk menangani subjek data yang terjejas?

SEKSYEN E: KOMUNIKASI DAN PEMBERITAHUAN

18. Adakah anda telah berkomunikasi atau berinteraksi secara langsung dengan pelaku ancaman yang disyaki atau sebenar?

☐ Ya

☐ Tidak

☐ Tidak berkenaan. Tiada pelaku ancaman yang terlibat.

19. Adakah anda akan memberitahu atau telah memberitahu mana-mana badan pengawal selia tempatan atau asing mengenai pelanggaran data peribadi ini?

☐ Ya. Badan pengawal selia yang dimaklumkan termasuk:

☐ Tidak

20. Adakah anda telah memberitahu subjek data yang terjejas tentang pelanggaran data peribadi itu?

☐ Ya. (Sila lampirkan salinan atau contoh pemberitahuan yang diberikan)

☐ Tidak, tetapi kami berhasrat untuk memaklumkan subjek data yang terjejas.

☐ Tidak. Kami tidak berhasrat untuk memberitahu subjek data yang terjejas. (Sila berikan justifikasi)

21. Jika anda menjawab 'Ya' bagi Soalan 20, bagaimanakah pemberitahuan kepada subjek data yang terjejas dibuat?

☐ Pemberitahuan secara langsung dan individu (contohnya, melalui e-mel kepada subjek data yang terjejas)

☐ Pengumuman awam (contohnya media sosial dan kenyataan media).

SEKSYEN F: LAIN-LAIN

22. Adakah terdapat maklumat tambahan berkaitan pelanggaran data peribadi ini?