KEMENTERIAN DIGITAL

GARIS PANDUAN PERLINDUNGAN DATA PERIBADI

DBN

PEMBERITAHUAN PELANGGARAN DATA

Versi 1.0

Tarikh Terbitan: 25 Februari 2025

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

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 setimpal, 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:

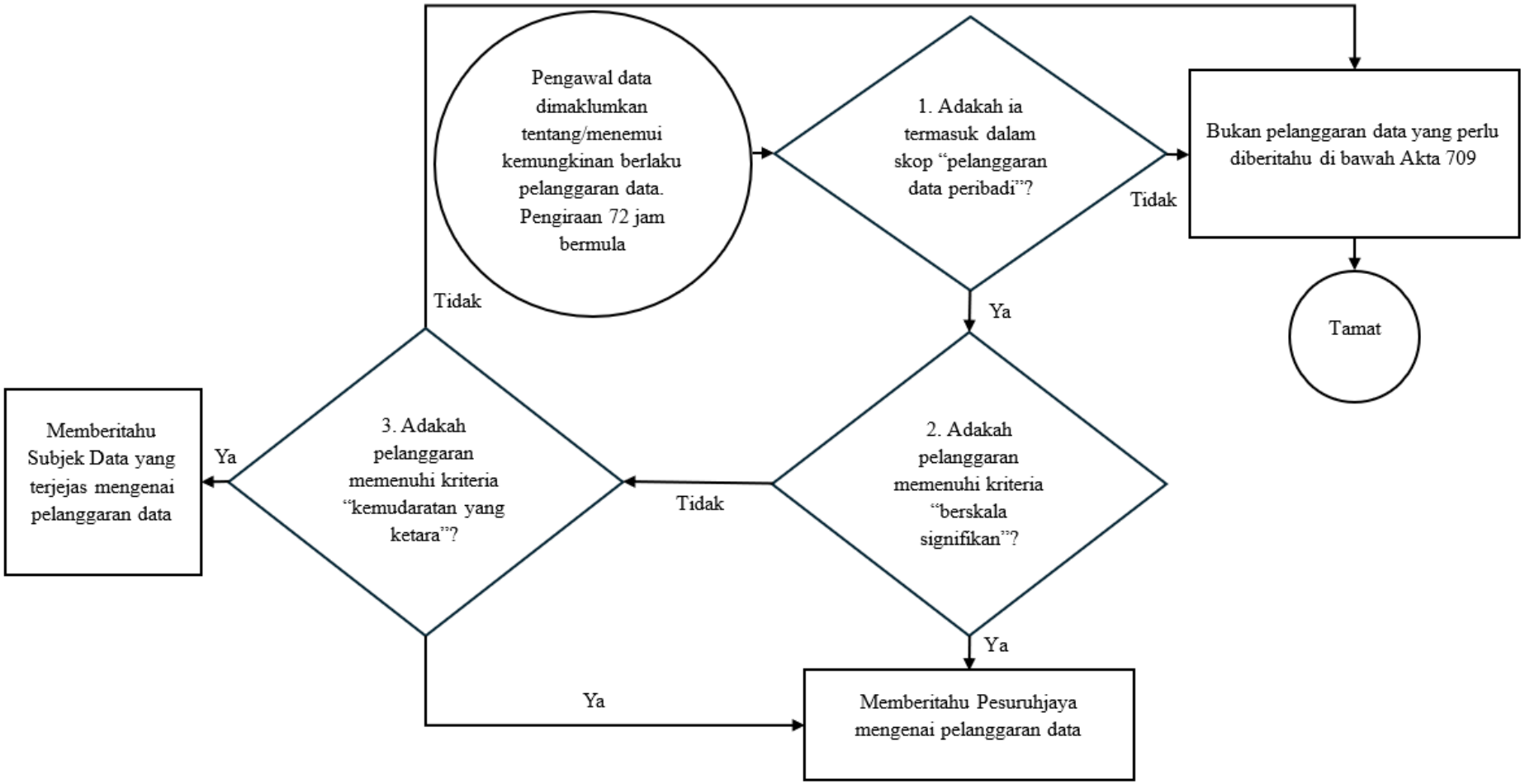
16.1.1 pemberitahuan kepada Polis Diraja Malaysia ("**PDRM**") yang mana pelanggaran data melibatkan aktiviti jenayah;

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?

MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION GUIDELINE

DBN

DATA BREACH NOTIFICATION

Version 1.0
Date of Issuance: 25 February 2025

Personal Data Protection Commissioner Malaysia

Address:

PERSONAL DATA PROTECTION COMMISSIONER OF MALAYSIA

Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana

Precinct 4, Federal Government Administration Centre

62100 Putrajaya, Malaysia

TABLE OF CONTENTS

PART A: INTRODUCTION

1 Background

1.1 Section 12B of the Personal Data Protection Act 2010 *[Act 709]* ("**Act 709**") introduces a mandatory requirement for data controller to notify the Personal Data Protection Commissioner ("**Commissioner**") and affected data subjects if the data controller has reasons to believe that a personal data breach has occurred.

1.2 This guideline sets out the procedure for data controller to notify the Commissioner and affected data subjects of a personal data breach, ensuring that such breaches are managed effectively and in compliance with the requirements of Act 709.

1.3 Please note that the examples provided in this Guideline are not intended to be exhaustive and are only included for context and for purposes of illustration.

1.4 This Guideline is to be read together with Act 709, Circular of Personal Data Protection Commissioner No. 2/2025 (Data Breach Notification) ("**Circular No. 2/2025**"), and any other relevant legislative instruments issued under the Act 709. This Guideline does not override any other specific data protection laws or data protection regulations in effect at any given time.

2 Legal Provisions

2.1 This Guideline is issued by the Commissioner pursuant to the functions of the Commissioner under subsection 48(g) of the Act 709.

2.2 In accordance with Section 12B(3) of the Act 709, any data controller who fails to comply with Section 12B(1) of the Act 709 shall, on conviction, be liable to a fine not exceeding two hundred and fifty thousand ringgit (RM250,000) or to imprisonment for a term not exceeding two (2) years or to both.

3 Interpretation

3.1 Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings assigned to them under the Act 709, the Circular No. 2/2025 and any other relevant legislative instruments under the Act 709.

3.2 In this Guideline, unless the context otherwise requires:

"security incident"	means an event or occurrence that affects or tends to affect data protection or may compromise the availability, confidentiality or integrity of data;
"personal data breach"	means as defined in section 4 of the Act 709 and is not limited to modification, duplication, alteration or destruction.

PART B: REQUIREMENTS FOR PERSONAL DATA BREACH NOTIFICATION TO THE COMMISSIONER

4 What Constitutes a "Personal Data Breach"?

4.1 The notification obligation under Act 709 only applies in the event of a "personal data breach" as defined by the Act 709 and the Circular No. 2/2025. Therefore, it is essential for a data controller to be able to recognise and determine what constitutes a "personal data breach".

4.2 A "personal data breach" broadly refers to any event / incident that leads or is likely to lead to the breach, loss, misuse or unauthorised access of personal data. A personal data breach may be caused by accidental or deliberate actions, either internally or externally.

Examples:

(i) Access to personal data held by the data controller by unauthorised third party.

(ii) An employee accidentally sending an email containing personal data to the wrong recipient.

(iii) An employee accidentally losing / misplacing a company-issued laptop containing unencrypted personal data, leading to potential unauthorised access of personal data.

(iv) An employee with authorised access to sensitive personal data deliberately stealing personal data (e.g., customer information) and selling it to a third party.

(v) An external party gaining access by unlawful means to the data controller's network or user accounts and extracting personal data.

(vi) A system misconfiguration leading to the loss of personal data or inadvertent sharing of personal data with third party.

(vii) The alteration of personal data without permission.

(viii) A temporary or permanent loss of availability of personal data (such as situations where unauthorised third party holds personal data hostage by preventing the data controller from gaining access to it, or situations where the corresponding decryption key to encrypted data has been lost).

(ix) An employee misplacing or losing physical documents containing personal data such as medical records, financial statements, etc., during transit or storage.

(x) An employee leaving personal data such as forms with identification details unattended on desks or in open areas where unauthorised individuals can view them.

(xi) The sending of letters or forms containing personal data such as invoices or financial statements to the wrong recipient.

5 Personal Data Breach that Must be Notified to the Commissioner

5.1 Not all personal data breaches are notifiable to the Commissioner. A data controller is only required to notify the Commissioner of a personal data breach if the personal data breach causes or is likely to cause "*significant harm*".

What is "significant harm"?

5.2 A personal data breach is considered to cause or is likely to cause "*significant harm*" if there is a risk that the compromised personal data:

5.2.1 may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;

5.2.2 may be misused for illegal purposes;

5.2.3 consists of sensitive personal data;

5.2.4 consists of personal data and other personal information which, when combined, could potentially enable identity fraud; or

5.2.5 is of significant scale.

What is "significant scale"?

5.3 A personal data breach is considered to be of *"significant scale"* if the number of affected data subjects exceeds one thousand (1,000).

Examples of Personal Data Breach

5.4 Examples of personal data breach scenarios, where the data controller is required to notify the Commissioner:

Example	**Whether Notification to the Commissioner is Required**
An employee loses a laptop containing personal data of customers.	Yes, if the type of datasets compromised are those that may result in "*significant harm*, or if the breach involves more than 1,000 affected data subjects.
Unauthorised third-party gains access to the medical records of patients.	Yes, because a breach involving "sensitive personal data" (i.e., medical records) is considered to be of "*significant harm*", regardless of whether the number of affected data subjects exceeds 1,000 data subjects.
Theft of an encrypted laptop containing the email addresses of 200 employees of an organisation.	No, the disclosure of the e-mail addresses of employees is not likely to result in any "*significant harm*".
Medical records in a hospital are temporarily inaccessible due to a cyberattack.	Yes, because a breach involving "sensitive personal data" (i.e., medical records) is considered to have the potential to cause "*significant harm*", regardless of whether the number of affected data subjects exceeds 1,000.
An e-mail containing the account statement of a customer was sent to the wrong recipient.	Yes, because the compromised personal data involves the financial information of a data subject.

5.5 The data controller shall assess whether a 'personal data breach' meets any of the notification criteria stipulated in paragraph 5.2. If any of the criteria is met, the data controller shall notify the Commissioner of the breach.

6 Timeframes for Notification to the Commissioner

6.1 The notification shall be made as soon as practicable and no later than seventy-two (72) hours from the occurrence of the personal data breach.

Computation of the 72-hour Timeframe for Notification

6.2 Once the data controller is informed by an individual, a media organisation, or any other source, or detects a security incident, he shall conduct a preliminary investigation to determine whether a personal data breach has actually occurred.

Examples:

The following are examples of the computation of the 72-hour timeframe for submission of data breach notification to the Commissioner:

(i) When a USB key containing unencrypted personal data is reported as lost, the 72-hour notification period to the Commissioner begins as soon as the data controller is informed of the loss.

(ii) The 72-hour notification period to the Commissioner begins as soon as the data controller unintentionally sends personal data without authorisation and realises the mistake."

(iii) In cases where a data controller's network is potentially compromised or infiltrated, the 72-hour notification period to the Commissioner begins as soon as the data controller confirms, during the inspection of their system, that the system has indeed been compromised.

(iv) A ransomware attack is a type of cyberattack in which criminals encrypt the victim's data and prevent them from accessing their system. The criminals then demand a ransom payment to restore the victim's access. In such cases, the 72-hour notification period to the Commissioner begins when the data controller realises he has lost access to the data or, after being informed by the cybercriminal of the breach, conduct own assessment and confirm that a personal data breach has occurred.

(v) Where a data processor processes data on behalf of a data controller, the 72-hour notification period to the Commissioner begins once the data processor notifies the data controller of the personal data breach or when the data controller itself obtains clear evidence that a personal data breach has occurred, whichever is earlier."

7 Notification Process to the Commissioner

Format and Channels of Notification

7.1 Notification to the Commissioner shall be made through one of the following channels:

7.1.1 completing the notification form available on the official website of the Department of Personal Data Protection (JPDP) at www.pdp.gov.my;

7.1.2 completing the notification form in **Annex B** and submitting it to the official e-mail address dbnpdp@pdp.gov.my; or

7.1.3 completing the notification form in **Annex B** and submitting a hard copy to the Commissioner.

Notification in Phases

7.2 The data controller shall ensure that all required / mandatory information fields in the notification form in paragraph 7.1 are completed, and that the notification to the Commissioner, through the methods specified in paragraph 7.1, is submitted within the prescribed seventy-two (72) hours.

7.3 The Commissioner will issue a confirmation notice to the data controller upon receiving the personal data breach notification. The notification will not be considered submitted to the Commissioner without this confirmation notice.

7.4 In addition to the required / mandatory fields in the notification form submitted under paragraph 7.1, the data controller shall also provide the Commissioner with the following information:

7.4.1 Details of the personal data breach, including:

7.4.1.1 the date and time the personal data breach was detected by the data controller;

7.4.1.2 the type of personal data involved and the nature of the breach;

7.4.1.3 the method used to identify the breach and the suspected cause of the incident;

7.4.1.4 the number of affected data subjects;

7.4.1.5 the estimated number of affected data records; and

7.4.1.6 the personal data system affected, which resulted in the breach;

7.4.2 the potential consequences arising from the personal data breach;

7.4.3 the chronology of events leading to the loss of control over personal data;

7.4.4 measures taken or proposed to be taken by the data controller to address the personal data breach, including steps implemented or planned to mitigate the possible adverse effects of the breach;

7.4.5 measures taken or proposed to be taken to address the affected data subjects; and

7.4.6 the contact details of the data protection officer or any other relevant contact person from whom further information on the personal data breach may be obtained.

7.5 Where and to the extent that it is not possible for the data controller to provide all the information requested in paragraph 7.4 at the time of submitting the initial notification to the Commissioner, the information may be provided in phases, as soon as practicable and no later than thirty (30) days from the date of the notification made under paragraph 7.1.

Personal Data Breach Involving Multiple Data Controllers

7.6 Where a personal data breach involves more than one (1) data controller, each data controller shall submit his own separate data breach notification to the Commissioner.

Delayed Data Breach Notification

7.7 Where the data controller fails to notify the Commissioner within seventy-two (72) hours, a written notice shall be submitted to the Commissioner, detailing the reasons for the delay and providing supporting evidence. The supporting evidence shall include documentation of the incident timeline, internal communications and any technical issues or external factors that contributed to the delay. All relevant documents shall be submitted together with the notification.

Contact Point and Assistance with the Commissioner's Investigations

7.8 Where the data controller is subject to the mandatory requirement to appoint data protection officer under Section 12A of the Act 709, the data protection officer shall act as the main point of contact for any inquiries or requests from the Commissioner regarding the personal data breach. Where the data controller is not subject to the mandatory requirement to appoint data protection officer, the data controller shall name or designate a representative with sufficient seniority and expertise to act as the point of contact.

7.9 In accordance with Section 105 of Act 709, the Commissioner may conduct an investigation into the data controller to determine whether any act, practice or request violates the provisions of Act 709.

7.10 The Commissioner may direct the data controller to submit records related to data breach notifications or any report documents upon request, in accordance with Section 121 of Act 709.

PART C: REQUIREMENTS FOR PERSONAL DATA BREACH NOTIFICATION / COMMUNICATION TO DATA SUBJECTS

8 Personal Data Breach that Must be Notified to Affected Data Subjects

8.1 The data controller shall notify data subjects of a personal data breach if the breach results in or is likely to result in "*significant harm*" to the data subjects.

8.2 Paragraph 5.2 which defines "significant harm" in the context of notifying the Commissioner, also applies when assessing whether a breach constitutes "significant harm" for the purpose of notifying data subjects. However, the "significant scale" criterion under paragraph 5.3 does not apply when determining whether notification to affected data subjects is required.

Examples of Personal Data Breach That Require Notification to the Affected Data Subjects

8.3 Examples of personal data breach scenarios where a data controller is required to notify the affected data subjects:

Example	**Whether Notification to the affected data subjects is Required**
A financial institution suffers a cyberattack which results in the theft of customers' personal and financial information including names, account numbers and passwords.	Yes, the risk of significant harm is high as a financial loss is likely to occur and the data includes information that may be used to enable identity fraud. As such, the data subjects would need to be informed about the breach.
A cybercriminal hacked the server which contains customers' personal and financial data and gained control of the pharmaceutical supplier's server. However, the cybercriminal is not able to access the said personal and financial data as the pharmaceutical supplier had implemented two layers of security measures.	No, in this situation, the data subjects do not need to be informed as the data is protected by security measures that render the information unintelligible or meaningless to the cybercriminal. However, the data controller needs to inform the Commissioner in the prescribed manner.
A cybercriminal circumvents the server security system of a direct seller and gains overall control of the data on the server. The cybercriminal threatens to delete the data on the server if the company does not pay a ransom. The direct seller does not have any backups of the said data.	Yes, in this situation, the data subjects need to be informed as there is a risk of loss of the personal and financial data of the data subjects.

9 Timeframes for Notification to Data Subjects

9.1 The notification to the affected data subjects, as referenced in paragraph 8.1, must be made without unnecessary delay, not later than seven (7) days after the initial data breach notification is made to the Commissioner under paragraph 7.1.

10 Manner of Notification to Affected Data Subjects

10.1 The notification to the affected data subjects shall be provided directly and individually to the data subjects in a practicable manner using intelligible language appropriate to the circumstances in order to allow the data subjects to take necessary precautions or other measures to protect themselves against the possible adverse effects of the breach.

Information to be Provided in Notification

10.2 The notification of a personal data breach by the data controller to the affected data subjects shall include the following information:

10.2.1 the details of the personal data breach that has occurred;

10.2.2 details on the potential consequences resulting from the personal data breach;

10.2.3 measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

10.2.4 measures that the affected data subjects may take to eliminate or mitigate any potential adverse effects resulting from the data breach; and

10.2.5 the contact details of the data protection officer or other contact point from whom more information regarding the personal data breach can be obtained.

Manner of Notification

10.3 If direct notification is not practicable or requires a disproportionate effort, the data controller may use alternative means of notification, such as public communication or any similar method that effectively informs affected data subjects of the personal data breach.

10.4 Examples of "*disproportionate effort*" include the following:

10.4.1 the data controller is required to contact a large number of data subjects across multiple states or countries, where doing so would result in an excessive logistical, administrative or financial burden; or

10.4.2 the data controller must notify data subjects who have provided outdated or incorrect contact information, where doing so would require extensive resources to obtain the correct contact details for each data subject.

Examples of methods for notifying affected data subjects individually:

- email;
- SMS;
- direct messaging; and
- postal communication.

Examples of public communication:

- notification on the official website;
- notice in printed media;
- social media posts through the data controller's official pages or accounts; and
- automated notifications (push notification).

10.5 The form of notification used to inform the affected data subjects of the personal data breach should be sent separately from other information, such as regular updates, newsletters or standard messages, so that the communication of the breach is clear and transparent.

11 Governance Requirements

11.1 Data controller shall put in place adequate data breach management and response plans.

11.2 The focus of any breach management and response plan should be on ensuring that the data controller is able to promptly identify a personal data breach, take appropriate measures to contain and mitigate the breach and ensure compliance with his data breach notification obligations.

11.3 The data breach management and response plan shall, at a minimum, outline policies and procedures to address the following:

11.3.1 personal data breach identification and escalation procedures;

11.3.2 roles and responsibilities of relevant stakeholders (e.g., the data breach response plan, the data protection officer);

11.3.3 steps to contain and mitigate the impact of the breach;

11.3.4 steps to determine whether it is necessary to notify the Commissioner and / or the affected data subjects;

11.3.5 communication plan for notifying the Commissioner and / or the affected data subjects; and

11.3.6 post-incident review.

11.4 Data controller should also conduct periodic training, as well as awareness and simulation exercises, in order to ensure that his employees are aware of their roles and responsibilities in assisting the data controller in responding to the personal data breach.

12 Personal Data Breach involving Data Processor

12.1 The mandatory personal data breach notification under Section 12B of the Act 709 does not directly apply to data processor.

12.2 The data controller is required to contractually impose an obligation on his data processor to promptly notify him about a data breach that has occurred, and to provide all reasonable and necessary assistance to the data controller to meet the data controller's data breach notification obligation under the Act 709.

13 Duty of Data Controller to Conduct Assessment of Data Breach

13.1 The data controller should act promptly as soon as he becomes aware of any personal data breach to assess, contain and reduce the potential impact of the data breach.

13.2 Investigating a data breach can be time-consuming and the data controller may not be able to obtain a complete understanding of the breach during the initial stages of the investigation, particularly if the breach is complex.

13.3 Once the data controller becomes aware of a personal data breach, he should consider the following immediate containment actions where applicable:

13.3.1 isolate and disconnect the compromised database or system from the network;

13.3.2 suspend or disable compromised access rights;

13.3.3 stop the practices identified as having caused the data breach; and

13.3.4 determine whether the lost data can be recovered or whether any immediate remedial action can be taken to minimise further harm caused by the breach.

13.4 During the initial investigation into a data breach, the data controller should identify the following information:

13.4.1 the type(s) of personal data involved;

13.4.2 the number of affected data subjects;

13.4.3 the systems, servers, databases, platforms and services affected;

13.4.4 the chronology of events leading to the data breach;

13.4.5 the severity of the data breach;

13.4.6 the root cause of the data breach, and whether it is still ongoing;

13.4.7 the harm and potential harm that may result from the data breach;

13.4.8 the measures that should be taken to contain the data breach, and mitigate its possible adverse effects; and

13.4.9 the remedial actions that should be taken to reduce the harm to affected data subjects.

13.5 The information above may also assist the data controller in determining whether external assistance (e.g., data protection experts or technical forensic specialists) is required to help him respond to and contain the personal data breach.

13.6 The data controller should conduct a post-breach evaluation to review the effectiveness of the data breach management and response plan, as well as his data protection practices and policies to prevent the recurrence of similar incidents.

14 Obligation to Maintain Records of Personal Data Breaches

14.1 The data controller shall keep records and maintain a register detailing personal data breach for a period of at least two (2) years from the date of the notification to the Commissioner, including those that did not meet the notification criteria for informing the Commissioner and/or affected data subjects. The register should, at a minimum, document the following information:

14.1.1 description of the personal data breach, including the date and time the data controller became aware of the personal data breach, an analysis and identification of the root cause, the type of personal data involved, the estimated number of affected data subjects, the estimated number of affected data records and the compromised personal data system which allowed the breach to occur;

14.1.2 description of the likely consequences of the personal data breach;

14.1.3 description of a chronology of the events leading to personal data breach;

14.1.4 containment and recovery measures taken to address the personal data breach; and

14.1.5 details of notifications made to the Commissioner and/or affected data subjects and justification for not making notifications, where applicable.

14.2 The data controller is free to determine what method and format to use when documenting the breach, provided that the documentation is in such a way that is clear, concise and enables the Commissioner to verify that the data controller has complied with this documentation requirement.

14.3 Documentation of the personal data breach under Paragraph 14.1 above shall be made available when requested by the Commissioner.

PART D: NOTIFICATION OBLIGATION UNDER OTHER LAWS

15 Duty to Comply with Other Applicable Notification Obligation under Malaysian Laws

15.1 The mandatory personal data breach notification obligation under Act 709 applies independently and concurrently with any other similar notification obligations that may be applicable to the data controller under existing laws and regulations in Malaysia.

15.2 The Data controller should identify the relevant notification requirements that may apply to him, as well as establish internal processes and procedures to facilitate compliance with the multiple notification requirements that may be applicable to him.

16 Notification Requirement under Other Malaysian Laws

16.1 Below is a non-exhaustive listing of notification requirements imposed under other Malaysian laws and regulations that may be applicable to the data controller:

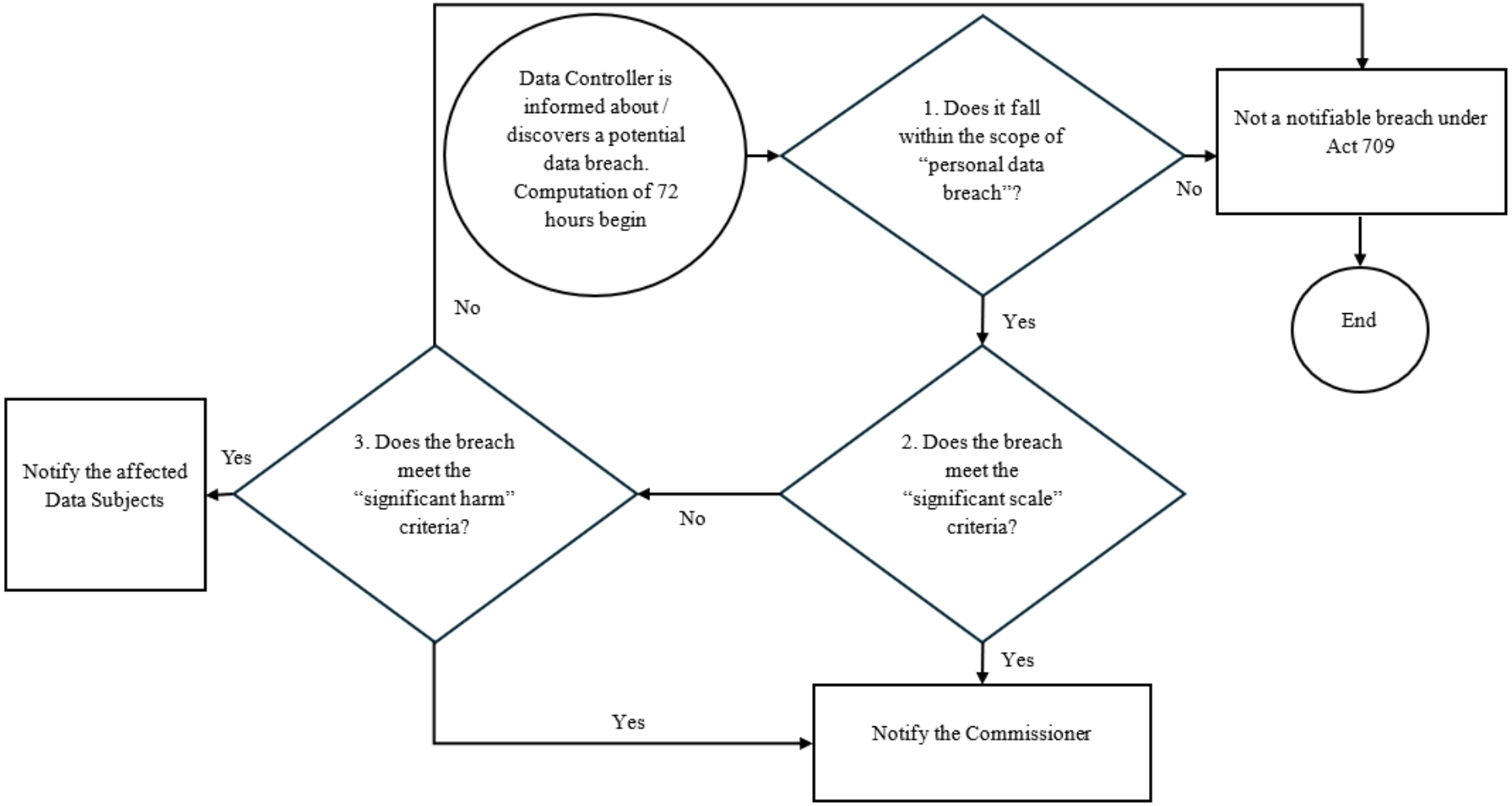
16.1.1 notification to the Royal Malaysia Police ("**PDRM**"), when the data breach involves criminal activity;

16.1.2 notification to sectoral regulators, such as Bank Negara Malaysia ("BNM"), Securities Commission Malaysia ("SC") and Malaysian Communications and Multimedia Commission ("MCMC"), pursuant to sectoral cyber incident or data breach notification requirements; and

16.1.3 notification to the Chief Executive of the National Cyber Security Agency ("NACSA") and National Critical Information Infrastructure ("NCII") Sector Leads ("NCII Sector Leads"), where the data controller is a designated NCII Entity under the Cyber Security Act 2024.

16.2 Please note that the list above is for reference purposes only. The data controller should conduct an independent assessment to determine the notification requirements under other applicable Malaysian laws and regulations.

ANNEX A: FLOWCHART OVERVIEW OF THE DATA BREACH NOTIFICATION REQUIREMENT UNDER THE ACT 709



ANNEX B: DATA BREACH NOTIFICATION FORM

DATA BREACH NOTIFICATION

This notification form is to be used when a data controller wishes to report a data breach to the Personal Data Protection Commissioner ("**Commissioner**").

Please note that the information requested in this notification form is non-exhaustive. The Commissioner may require further details of the incident to facilitate investigation.

Where and to the extent that it is not possible to provide all of the information requested in the notification form, is sufficient to complete the form only to the extent of the information available. Additional information to the Commissioner in phases as soon as practicable not later than thirty (30) days from the date of the initial notification.

PARTICULARS OF DATA CONTROLLER

Organisation : ----------

Address : ----------

Contact person

Name : ----------

Designation : ----------

Telephone Number : ----------

Email : ----------

Date : ----------

Signature : ----------

Based on the information you have provided, we will contact you to inform about our next steps. All personal data submitted will only be used for purposes which are directly related to this notification and the exercise of the regulatory powers and functions of the Commissioner.

Submission of notification:

PERSONAL DATA PROTECTION COMMISSIONER
8th Floor, Galeria PjH, Jalan P4W
Persiaran Perdana, Presint 4
62100 W.P Putrajaya
or via email: dbnpdp@pdp.gov.my

SECTION A: BASIC INFORMATION

1. Is this a new notification or an update to a previous notification that has been submitted to the Commissioner?

☐ New notification

☐ Update. Please indicate the reference number of the original notification:

2. If this is a new notification, are you submitting it within the 72 hours after becoming aware of the personal data breach?

☐ Yes

☐ No. Please provide the reason(s) for the delay with supporting evidence:

SECTION B: DETAILS OF THE PERSONAL DATA BREACH

3. When did your organisation become aware of the personal data breach?
(Please include the date and time of when your organisation became aware of the breach)

Date :	*Time :*

4. How did your organisation become aware of the personal data breach?
(Please provide a brief explanation of how your organization detected the personal data breach)

5. How was personal data affected or compromised?

(Select all that apply)

☐ Data was disclosed to unintended parties

☐ Data was lost

☐ Data was temporarily unavailable

☐ Data was exfiltrated / stolen

☐ Unauthorised access of personal data

☐ Others:

6. What is the actual or suspected cause of the incident?

(Select only one)

☐ Cyber incident

☐ Human error

☐ System error

☐ Theft / misuse of information by malicious actors

☐ Others:

7. How was the actual cause of the above incident identified? (Please specify)

8. Which system or application was affected in this personal data breach incident? (Please specify)

9. Where is the storage location of the personal data affected by this personal data breach?

☐ Malaysia

☐ Other jurisdictions (Please specify)

10. What is the status of the personal data breach incident?

☐ In Progress

☐ Rectified / Contained

11. Are there any other parties affected by the personal data breach (e.g., other data controllers or data processors)?

☐ No.

☐ Yes. Please list out these parties:

SECTION C: DETAILS OF COMPROMISED DATA

12. What types of personal data were compromised?

13. Number of data subjects affected or potentially affected?

14. Does this personal data breach only affect data subjects who are Malaysian citizens?

☐ Yes.

☐ No. The breach also affects data subjects in the following jurisdictions:

15. What harm or risks may result from the personal data breach affecting data subjects?

☐ Physical harm to threat to safety

☐ Financial loss

☐ Identity theft or fraud

☐ Misuse of data for unlawful purposes

☐ Data contains sensitive data

☐ Data contains financial information

☐ No potential harm to data subjects

☐ Others (Please specify)

SECTION D: CONTAINMENT AND RECOVERY ACTIONS

16. What actions have been or will be taken to contain and mitigate the harm or risks arising from the breach?

17. **What actions have been or will be taken to address the affected data subjects?**

SECTION E: COMMUNICATION AND NOTIFICATION

18. **Have you communicated or directly interacted with the suspected or actual threat actor?**

☐ Yes

☐ No

☐ Not applicable. There are no threat actor is involved.

19. **Have you notified or will you notify any local or foreign regulatory bodies regarding this personal data breach?**

☐ Yes. These regulatory bodies include:

☐ No

20. **Have you notified the affected data subjects about the personal data breach?**

☐ Yes. (Please attach a copy or sample of the notification provided)

☐ No, but we intend to notify the affected data subjects.

☐ No. We do not intend to notify the affected data subjects. (Please provide justifications)

21. If you answered "Yes" to Question 20, how was the notification to the affected data subjects made?

☐ Direct and individual notification (e.g., via email to affected data subjects).

☐ Public announcement (e.g., social media and press release).

SECTION F: OTHERS

22. Is there any additional information related to this personal data breach?
