KEMENTERIAN DIGITAL

GARIS PANDUAN
PERLINDUNGAN DATA PERIBADI

PELANTIKAN PEGAWAI PERLINDUNGAN 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 12A Akta Perlindungan Data Peribadi 2010 [*Akta 709*] ("**Akta 709**") memperuntukkan keperluan kepada pengawal data dan pemproses data untuk melantik seorang atau lebih pegawai perlindungan data dalam memastikan pematuhan terhadap Akta 709.

1.2 Garis panduan ini bertujuan untuk menjelaskan keperluan pelantikan, tugas dan tanggungjawab pegawai perlindungan data serta kewajipan pengawal data dan pemproses data dalam memastikan pelaksanaan peranan pegawai perlindungan data yang berkesan selaras dengan peruntukan Akta 709.

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

1.4 Garis Panduan ini hendaklah dibaca bersama dengan Akta 709, Pekeliling Pesuruhjaya Perlindungan Data Peribadi Bilangan 1 Tahun 2025 (Pelantikan Pegawai Perlindungan Data) ("**Pekeliling Bil. 1/2025**") 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 Perlindungan Data Peribadi ("**Pesuruhjaya**") adalah selaras dengan fungsi Pesuruhjaya di bawah subseksyen 48(g) Akta 709.

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. 1/2025 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:

"maklumat hubungan perniagaan"	ertinya nama individu, jawatan atau gelaran, nombor telefon perniagaan, alamat perniagaan, alamat e-mel perniagaan atau nombor faks perniagaan dan sebarang maklumat lain yang sempurna tentang individu tersebut, tidak diberikan oleh individu itu semata-mata untuk tujuan peribadinya.

BAHAGIAN B: SYARAT-SYARAT PELANTIKAN PEGAWAI PERLINDUNGAN DATA

4 Syarat-syarat bagi Pelantikan Pegawai Perlindungan Data

4.1 Di bawah Pekeliling Bil. 1/2025, pelantikan pegawai perlindungan data adalah tertakluk kepada syarat-syarat yang ditentukan oleh Pesuruhjaya.

4.2 Bagi maksud seksyen 12A Akta 709, pengawal data dan pemproses data hendaklah melantik seorang atau lebih pegawai perlindungan data dalam mana-mana kes jika pemprosesan melibatkan:

4.2.1 data peribadi melebihi 20,000 bilangan subjek data;

4.2.2 data peribadi yang sensitif termasuk maklumat kewangan melebihi 10,000 subjek data; atau

4.2.3 melibatkan aktiviti yang memerlukan pemantauan data peribadi secara berkala dan sistematik.

4.3 Bagi tujuan menentukan "*pemantauan berkala dan sistematik*" dalam perenggan 4.2.3 di atas, berikut adalah contoh sebagai rujukan:

Contoh:

- Sebarang bentuk aktiviti yang melibatkan pengesanan dan pemprofilan subjek data dalam talian atau luar talian untuk tujuan pengiklanan tingkah laku akan dianggap sebagai aktiviti yang memerlukan pemantauan berkala dan sistematik.

- Laman sesawang runcit yang menggunakan algoritma untuk memantau carian dan pembelian penggunanya dan berdasarkan maklumat ini, menawarkan cadangan kepada mereka akan dianggap menjalankan "*pemantauan berkala dan sistematik*" subjek data.

- Pengawal data atau pemproses data yang menjalankan aktiviti seperti:

    - mengendalikan rangkaian telekomunikasi;
    - memantau keafiatan, kecergasan dan data kesihatan melalui peranti boleh pakai; dan / atau
    - aktiviti yang melibatkan sistem kamera litar tertutup (CCTV) atau peranti terhubung seperti kereta pintar, sistem automasi rumah dan sebagainya,

  merupakan aktiviti yang dianggap sebagai “pemantauan berkala dan sistematik”.

- Pengurusan program kesetiaan (*loyalty program*) mungkin tidak dianggap sebagai aktiviti yang memerlukan "pemantauan berkala dan sistematik" terhadap subjek data sekiranya program tersebut hanya bertujuan untuk mengurus akaun subjek data dan bukan untuk memantau tingkah laku pembelian mereka.

4.4 Walau apa pun perenggan 4.2, pengawal data atau pemproses data hendaklah memberitahu tentang pelantikan pegawai perlindungan data kepada Pesuruhjaya sekiranya terdapat apa-apa keperluan yang mendesak.

4.5 Pengawal data atau pemproses data boleh menyimpan rekod alasan untuk tidak melantik pegawai perlindungan data sekiranya mendapati syarat-syarat dalam perenggan 4.2 tidak dipenuhi.

5 Kemahiran atau Kepakaran Pegawai Perlindungan Data

5.1 Pengawal data atau pemproses data perlu memastikan bahawa pegawai perlindungan data yang dilantik dapat melaksanakan tugas mereka dengan sewajarnya.

5.2 Tertakluk kepada perenggan 5.6 dan 5.7 di bawah, pengawal data dan pemproses data hendaklah menentukan tahap kelayakan yang bersesuaian, pengalaman, kemahiran dan kepakaran yang diperlukan untuk pegawai perlindungan data dengan mengambil kira:

5.2.1 operasi pemprosesan data peribadi yang dijalankan;

5.2.2 kerumitan dan skala data yang diproses;

5.2.3 sensitiviti data peribadi yang diproses; dan

5.2.4 tahap perlindungan yang diperlukan untuk data yang diproses.

5.3 Pegawai perlindungan data yang dilantik perlu memiliki tahap kemahiran atau kepakaran yang lebih tinggi serta sokongan daripada pengawal data atau pemproses data, bergantung kepada faktor-faktor seperti:

5.3.1 skala data peribadi sensitif yang diproses; atau

5.3.2 terlibat dalam pemprosesan data peribadi yang kompleks seperti perkongsian data peribadi secara sistematik antara beberapa organisasi dan pemindahan data peribadi rentas sempadan.

Kemahiran atau Kepakaran Minimum

5.4 Tiada penetapan bagi kelayakan kepakaran profesional minimum yang diperlukan sebelum dilantik sebagai pegawai perlindungan data melainkan pengawal data atau pemproses data atau Pesuruhjaya menentukan sebaliknya dari semasa ke semasa.

5.5 Walau apa pun, pengawal data atau pemproses data perlu memastikan bahawa pegawai perlindungan data yang dilantik boleh menunjukkan tahap kebolehan dalam kemahiran, kualiti dan kepakaran yang berikut:

5.5.1 pengetahuan mengenai Akta 709, keperluan di bawah undang-undang dan amalan perlindungan data negara (termasuk mana-mana undang-undang perlindungan data yang relevan dan berkaitan);

5.5.2 pemahaman mengenai operasi perniagaan pengawal data atau pemproses data dan operasi pemprosesan data peribadi yang dijalankan;

5.5.3 pemahaman mengenai teknologi maklumat dan keselamatan data;

5.5.4 kualiti peribadi seperti integriti, pemahaman tentang tadbir urus korporat dan etika profesional yang tinggi;

5.5.5 keupayaan untuk menggalakkan budaya perlindungan data dalam organisasi.

Latihan Pegawai Perlindungan Data

5.6 Bagi memastikan pegawai perlindungan data yang dilantik mempunyai pengetahuan, kemahiran dan kepakaran yang diperlukan untuk melaksanakan tugas-tugas mereka dengan cekap, Pesuruhjaya boleh menentukan mekanisme yang perlu atau suai manfaat seperti menetapkan kursus dan program latihan termasuk mekanisme penanda aras kemahiran profesional perlindungan data serta program lain berkaitan untuk pegawai perlindungan data.

5.7 Pengawal data atau pemproses data hendaklah memastikan bahawa pegawai perlindungan data yang dilantik mempunyai latihan dan kemahiran yang mencukupi untuk melaksanakan tanggungjawab pegawai perlindungan data dengan berkesan dengan menghadiri kursus dan program latihan yang berkaitan.

6 Perkara Berkaitan dengan Pelantikan Pegawai Perlindungan Data

6.1 Pelantikan pegawai perlindungan data tidak melepaskan pengawal data atau pemproses data daripada obligasi untuk memastikan pematuhan terhadap keperluan Akta 709 semasa memproses data peribadi. Pengawal data atau pemproses data kekal bertanggungjawab dan dipertanggungjawabkan ke atas sebarang ketidakpatuhan terhadap peruntukan di bawah Akta 709.

6.2 Seorang pegawai perlindungan data boleh melaksanakan tugas dan tanggungjawab rasmi yang lain atau melaksanakan tugasan tambahan sebagai sebahagian daripada skop kerja seperti pegawai undang-undang, pegawai pengurusan risiko dan lain-lain. Walau bagaimanapun, pengawal data atau pemproses data hendaklah memastikan bahawa pelaksanaan kerja dan fungsi lain tersebut tidak mengakibatkan pencanggahan kepentingan kepada pegawai perlindungan data.

Contoh:

- Seorang Ketua Pemasaran bagi pengawal data atau pemproses data diminta untuk menjalankan kempen pemasaran bagi mempromosikan produk dan menerima peranan kedua sebagai pegawai perlindungan data dalam syarikat. Ketua Pemasaran tersebut sewajarnya tidak menerima peranan pegawai perlindungan data kerana objektif mereka untuk:

  (i) menyasarkan seramai mungkin pelanggan dan memproses data peribadi mereka untuk tujuan pemasaran langsung; dan

  (ii) memaksimumkan jualan produk mungkin bercanggah dengan peranan pegawai perlindungan data dalam organisasi untuk memastikan pematuhan Akta 709 dan melindungi data peribadi pelanggan.

- Peranan seperti pengurus rekod atau pegawai pematuhan secara amnya mungkin kurang menimbulkan konflik kepentingan kerana tumpuan peranan-peranan ini adalah untuk memastikan pematuhan terhadap hak-hak perlindungan data peribadi.

6.3 Pegawai perlindungan data boleh dilantik sama ada secara separa masa atau sepenuh masa dengan mengambil kira fungsi organisasi, struktur dan saiz.

6.4 Sekiranya individu yang dilantik sebagai pegawai perlindungan data memberhentikan perkhidmatannya/tamat tempoh perkhidmatan, pengawal data atau pemproses data hendaklah melantik, melantik semula atau mengambil pengganti baharu dalam tempoh masa yang munasabah. Pengawal data dan pemproses data hendaklah dengan seberapa segera melantik seorang pegawai perlindungan data interim untuk memantau komunikasi yang dihantar melalui alamat e-mel perniagaan rasmi pegawai perlindungan data.

Kaedah Pelantikan Pegawai Perlindungan Data

6.5 Pegawai perlindungan data boleh dilantik dalam kalangan pekerja sedia ada atau menggunakan perkhidmatan penyumberluaran (berdasarkan kontrak perkhidmatan yang ditandatangani dengan individu atau organisasi).

6.6 Sekiranya pegawai perlindungan data dilantik melalui kontrak, pengawal data atau pemproses data disyorkan untuk memastikan pelantikan tersebut adalah untuk tempoh sekurang-kurangnya dua (2) tahun bagi memastikan kestabilan.

6.7 Pengawal data atau pemproses data yang melantik pegawai perlindungan data menggunakan perkhidmatan penyumberluaran hendaklah menerangkan dengan jelas, ringkas dan menyeluruh mengenai kewajipan dan obligasi pegawai perlindungan data dalam kontrak perkhidmatan tersebut.

6.8 Pengawal data atau pemproses data hendaklah memastikan organisasi yang menyediakan perkhidmatan penyumberluaran melantik individu dalam organisasi sebagai hubungan utama dan orang yang bertanggungjawab ("**PIC**") untuk berhubung dengan pengawal data atau pemproses data tersebut. Hubungan utama atau PIC ini perlu dinyatakan / dirujuk dalam kontrak perkhidmatan dengan organisasi penyumberluaran tersebut.

Kebolehcapaian Pegawai Perlindungan Data

6.9 Seorang pegawai perlindungan data boleh dilantik untuk berkhidmat kepada beberapa pengawal data atau pemproses data dengan syarat pegawai perlindungan data tersebut mudah dihubungi oleh entiti-entiti berlainan yang menerima khidmat pegawai perlindungan data tersebut.

6.10 Untuk kebolehcapaian dan kecekapan maklum balas yang lebih baik, pegawai perlindungan data perlu:

6.10.1 bermastautin di Malaysia (iaitu berada secara fizikal di Malaysia untuk sekurang-kurangnya 180 hari dalam satu tahun kalendar); atau

6.10.2 mudah dihubungi melalui apa-apa cara; dan

6.10.3 mahir dalam Bahasa Kebangsaan dan Bahasa Inggeris.

7 Pemberitahuan Pelantikan Pegawai Perlindungan Data

7.1 Pengawal data yang memenuhi syarat-syarat pelantikan pegawai perlindungan data hendaklah mendaftarkan pegawai perlindungan data yang dilantik dan mengemukakan maklumat hubungan perniagaan pegawai perlindungan data dalam tempoh dua puluh satu (21) hari dari tarikh pelantikan.

7.2 Pemberitahuan kepada Pesuruhjaya mengenai pelantikan pegawai perlindungan data hendaklah dibuat melalui Sistem Perlindungan Data Peribadi (SPDP) di pautan https://daftar.pdp.gov.my.

7.3 Maklumat hubungan perniagaan hendaklah disenggara dengan sewajarnya dan dikemas kini dengan segera oleh pengawal data untuk memastikan komunikasi yang efisien dengan pegawai perlindungan data boleh dilaksanakan pada setiap masa yang munasabah.

7.4 Sekiranya terdapat perubahan pada maklumat pegawai perlindungan data yang dilantik atau maklumat hubungan perniagaan pegawai perlindungan data, pengawal data hendaklah segera menyenggara dan mengemaskini perubahan tersebut tidak lewat daripada empat belas (14) hari dari tarikh kuat kuasa pelantikan baharu melalui SPDP.

BAHAGIAN C: PERANAN PEGAWAI PERLINDUNGAN DATA

8 Tanggungjawab Pegawai Perlindungan Data berkaitan dengan Pengawal Data atau Pemproses Data yang Melantik

8.1 Dalam melaksanakan tugas, pegawai perlindungan data hendaklah mengambil pendekatan berasaskan risiko untuk menilai risiko dalam perspektif operasi pemprosesan pengawal data atau pemproses data dengan mengambil kira sifat, skop, konteks dan tujuan pemprosesan serta menyelaras dan bekerjasama dengan kakitangan lain mengikut keperluan.

8.2 Pegawai perlindungan data hendaklah sekurang-kurangnya mempunyai tanggungjawab teras berkenaan aktiviti-aktiviti pemprosesan data pengawal data atau pemproses data seperti berikut:

8.2.1 memaklumkan dan memberi nasihat kepada pengawal data atau pemproses data berkenaan pemprosesan data peribadi;

Contoh:

- mendidik pengawal data atau pemproses data mengenai keperluan yang terpakai di bawah Akta 709 berhubung aktiviti-aktiviti pemprosesan data peribadi.

- menasihati pengawal data atau pemproses data mengenai undang-undang, peraturan-peraturan dan instrumen-instrumen lain yang berkaitan, termasuk piawaian industri dan pensijilan bagi memastikan pematuhan yang mencukupi terhadap keperluan perlindungan data peribadi.

8.2.2 menyokong pengawal data atau pemproses data dalam mematuhi Akta 709 dan undang-undang perlindungan data lain yang berkaitan termasuk cakna terhadap risiko pemprosesan data yang melibatkan pengawal data atau pemproses data;

Contoh:

- mengumpul maklumat untuk mengenal pasti operasi pemprosesan, aktiviti, langkah, dasar atau sistem pengawal data atau pemproses data dan menyenggara rekod berkenaannya.

- menasihati dan menyelia pelaksanaan langkah-langkah keselamatan untuk melindungi data peribadi daripada akses, penzahiran, pengubahan atau pemusnahan tanpa kebenaran, selaras dengan keperluan undang-undang dan polisi keselamatan dalaman.

- menasihati pengawal data atau pemproses data tentang potensi risiko dan impak yang mungkin timbul daripada amalan perniagaan pengawal data atau pemproses data.

- membangun, mengkaji dan/atau menyemak dasar perlindungan data, garis panduan dan lain-lain.

- mempertimbang pengambilan pentauliahan atau pensijilan untuk menunjukkan standard pemprosesan data peribadi yang dilaksanakan oleh pengawal data atau pemproses data.

- menasihati pengawal data atau pemproses data tentang keperluan melaksanakan perjanjian yang mengikat dengan pihak ketiga (contohnya perjanjian pemindahan data, perjanjian sub pemprosesan dan lain-lain).

8.2.3 menyokong pelaksanaan Penilaian Impak Perlindungan Data mengikut keperluan yang ditentukan oleh Pesuruhjaya dari semasa ke semasa;

8.2.4 memantau pematuhan data peribadi pengawal data atau pemproses data;

Contoh:

- menganalisis dan menyiasat pematuhan aktiviti pemprosesan pengawal data atau pemproses data.

- menugaskan dan mewakilkan tanggungjawab-tanggungjawab di bawah dasar perlindungan data pengawal data atau pemproses data untuk menggalakkan kebertanggungjawapan dan penyeliaan yang menyeluruh.

- meningkatkan kesedaran dan melatih pekerja pengawal data atau pemproses data mengenai keperluan-keperluan perlindungan data.

- menjalankan audit ke atas pematuhan pengawal data atau pemproses data terhadap dasar dan keperluan perlindungan data.

- mengeluarkan syor untuk menutup apa-apa jurang pematuhan yang telah dikenal pasti.

8.2.5 memastikan pengurusan pelanggaran data dan insiden keselamatan dengan betul termasuk membantu pengawal data atau pemproses data untuk menyedia, memproses dan menyerahkan laporan serta dokumentasi lain yang diperlukan oleh Pesuruhjaya berkaitan pelanggaran data peribadi dalam tempoh yang telah ditetapkan; dan

8.2.6 tanggungjawab tambahan oleh Pesuruhjaya atau pengawal data atau pemproses data dari semasa ke semasa (contohnya hasil daripada perkembangan teknologi).

9 Tanggungjawab Pegawai Perlindungan Data berkaitan dengan Subjek Data

9.1 Pegawai perlindungan data hendaklah bertindak sebagai fasilitator dan titik penghubung di antara subjek data dan pengawal data atau pemproses data berkenaan dengan pemprosesan data peribadi subjek data serta hak-hak mereka.

Contoh:

- mengendalikan isu-isu berkaitan dengan pemprosesan data peribadi subjek data (contoh: aduan).

- mengendalikan permintaan berkenaan pelaksanaan hak subjek data (contoh: permintaan untuk membetulkan dan mengakses data peribadi).

- mendidik subjek data berkenaan pemprosesan data peribadi mereka (contoh: memaklumkan Subjek Data tentang tujuan pemprosesan data peribadi, pihak ketiga data peribadi mereka dizahirkan dan hak-hak subjek data).

- bertindak sebagai titik hubungan bagi subjek data dalam kes-kes pelanggaran data peribadi dan menangani apa-apa kebimbangan yang mungkin timbul daripada subjek data.

10 Tanggungjawab Pegawai Perlindungan Data berkaitan dengan Pesuruhjaya

10.1 Pegawai perlindungan data hendaklah bertindak sebagai pegawai perhubungan dan sumber rujukan utama pengawal data atau pemproses data dengan Pesuruhjaya.

Contoh:

- berfungsi sebagai pegawai perhubungan utama di antara pengawal data atau pemproses data dan Pesuruhjaya.

- memudahkan akses kepada dokumen dan maklumat ketika Pesuruhjaya menjalankan pemeriksaan atau penyiasatan terhadap aktiviti pemprosesan data peribadi oleh pengawal data atau pemproses data.

- menyedia dan mengemukakan maklumat berkenaan apa-apa pelanggaran data peribadi yang diperlukan oleh Pesuruhjaya mengikut garis masa yang ditetapkan.

- mewakili pengawal data atau pemproses data dalam sesi libat urus bersama industri atau program yang dianjurkan oleh Pesuruhjaya.

11 Kebebasan Pegawai Perlindungan Data

11.1 Pengawal data atau pemproses data hendaklah memastikan pegawai perlindungan data diberikan sumber-sumber yang diperlukan seperti di perenggan 14 Garis Panduan ini bagi membolehkan mereka melaksanakan fungsi-fungsi dengan kebebasan dan autonomi yang mencukupi.

11.2 Untuk memelihara kebebasan pegawai perlindungan data, pengawal data atau pemproses data hendaklah berusaha untuk mengelakkan pegawai perlindungan data berada dalam kedudukan yang boleh mengakibatkan konflik di antara kepentingan perniagaan dan pematuhan terhadap Akta 709.

11.3 Pegawai perlindungan data harus mempunyai akses pelaporan terus kepada pengurusan kanan tertinggi (atau setara) pengawal data atau pemproses data.

12 Tempoh Perkhidmatan Pegawai Perlindungan Data

12.1 Pegawai perlindungan data bertanggungjawab kepada pengawal data atau pemproses data yang telah melantik pegawai perlindungan data tersebut untuk mematuhi Akta 709.

12.2 Pegawai perlindungan data tidak sepatutnya dipecat oleh pengawal data atau pemproses data kerana telah melaksanakan tugasnya dengan suci hati, melainkan pegawai perlindungan data tersebut telah melanggar undang-undang yang berkenaan dan/atau didapati telah melakukan kecuaian atau salah laku.

BAHAGIAN D: TANGGUNGJAWAB PENGAWAL DATA DAN PEMPROSES DATA

13 Penglibatan Pegawai Perlindungan Data

13.1 Pengawal data atau pemproses data hendaklah memastikan penglibatan pegawai perlindungan data dalam semua isu yang berkaitan dengan perlindungan data peribadi dalam jangka waktu yang tepat.

13.2 Untuk memastikan bahawa Pegawai Perlindungan Data terlibat dalam masa yang tepat, pengawal data atau pemproses data hendaklah melibatkan Pegawai Perlindungan Data dalam semua perkara yang berkaitan dengan perlindungan data, bermula dari peringkat yang paling awal dalam kitaran hayat pemprosesan data, iaitu daripada penggubalan dasar sehingga pengumpulan, penyimpanan, dan pemadaman atau pemusnahan data peribadi.

Contoh:

- Pegawai perlindungan data wajar dilibatkan dalam mesyuarat pengurusan kanan / lembaga pengarah atau kumpulan kerja yang berkaitan untuk membincangkan tadbir urus perlindungan data peribadi di seluruh organisasi pengawal data atau pemproses data.
- Pegawai perlindungan data mesti diberikan maklumat yang diperlukan dan mencukupi dengan segera bagi membolehkan fungsi-fungsi mereka dilaksanakan dengan berkesan.
- Pandangan pegawai perlindungan data hendaklah diperoleh sebaik sahaja aktiviti organisasi dianggap berkemungkinan mempunyai implikasi terhadap atau terjejas oleh aktiviti pemprosesan data dalam organisasi pengawal data atau pemproses data.
- Pegawai Perlindungan Data mesti dimaklumkan dan dirujuk dengan segera apabila berlakunya pelanggaran data atau insiden keselamatan yang seumpama.

13.3 Sebagai amalan yang disyorkan, pengawal data atau pemproses data boleh membangunkan garis panduan perlindungan data sebagai tambahan kepada polisi keselamatan yang menggariskan senario di mana penglibatan pegawai perlindungan data diperlukan dan menyebarkan garis panduan ini di seluruh organisasi.

14 Penyediaan Sumber kepada Pegawai Perlindungan Data

14.1 Pengawal data atau pemproses data perlu memastikan bahawa pegawai perlindungan data diberikan sumber-sumber yang mencukupi untuk menjalankan tugas-tugas mereka dengan berkesan.

14.2 Apabila menilai kecukupan sumber-sumber untuk diberikan kepada pegawai perlindungan data, pengawal data atau pemproses data wajar mempertimbangkan faktor-faktor seperti kerumitan operasi pemprosesan data, sensitiviti data peribadi yang diproses serta saiz dan struktur organisasi pengawal data atau pemproses data.

14.3 Sumber-sumber yang mungkin disediakan oleh pengawal data atau pemproses data untuk menyokong fungsi-fungsi pegawai perlindungan data hendaklah dipertimbangkan secara menyeluruh.

Contoh:

Contoh sumber-sumber / sokongan yang mungkin diterima oleh pegawai perlindungan data daripada pengawal data atau pemproses data adalah seperti berikut :

- Pegawai perlindungan data menerima sokongan daripada pengurusan tertinggi dan lembaga pengarah dalam melaksanakan fungsi dan tanggungjawabnya.

- Pegawai perlindungan data diperuntukkan masa yang mencukupi untuk melaksanakan tugasnya, dengan mengambil kira pelantikannya adalah secara separa masa atau sepenuh masa, serta sama ada pegawai perlindungan data menjalankan tugas lain selain daripada tugas yang telah ditetapkan bagi peranannya.

- Pegawai perlindungan data diberikan akses kepada perkhidmatan lain seperti sumber manusia, perundangan, teknologi maklumat, keselamatan dan lain-lain bagi memastikan mereka menerima sokongan, input dan maklumat yang diperlukan daripada perkhidmatan tersebut.

- Pegawai perlindungan data diberikan sokongan yang mencukupi dalam bentuk sumber kewangan, infrastruktur (premis, kemudahan, peralatan) dan tenaga kerja. Bergantung kepada saiz dan struktur organisasi, mungkin terdapat keperluan untuk menubuhkan pasukan sokongan yang diketuai oleh pegawai perlindungan data bagi memastikan pelaksanaan fungsi dan tanggungjawabnya dapat dilaksanakan dengan berkesan.

- Pengawal data atau pemproses data secara rasmi mengiktiraf peranan pegawai perlindungan data dengan mengeluarkan notis kepada semua kakitangan dalam organisasi bagi memastikan kewujudan serta fungsi pegawai perlindungan data diketahui dan difahami.

- Pengawal data atau pemproses data memberikan latihan yang diiktiraf secara berterusan kepada pegawai perlindungan data bagi memastikan pembangunan profesional.

15 Penerbitan dan Komunikasi Maklumat Hubungan Pegawai Perlindungan Data

15.1 Pengawal data dan pemproses data hendaklah mewujudkan satu akaun e-mel perniagaan rasmi yang khusus untuk pegawai perlindungan data. Akaun e-mel perniagaan rasmi tersebut hendaklah diselenggara secara aktif sepanjang masa bagi memastikan komunikasi yang jelas, berkesan dan difahami di antara pegawai perlindungan data, Pesuruhjaya dan subjek data. Akaun e-mel perniagaan rasmi khusus yang diwujudkan hendaklah berbeza dan berasingan daripada alamat e-mel peribadi dan alamat e-mel rasmi perniagaan individu yang dilantik sebagai pegawai perlindungan data.

15.2 Pengawal data atau pemproses data hendaklah menerbitkan maklumat hubungan perniagaan pegawai perlindungan data melalui mana-mana atau semua kaedah / saluran berikut:

15.2.1 laman sesawang rasmi dan media rasmi lain;

15.2.2 notis perlindungan data peribadi;

15.2.3 dasar keselamatan dan garis panduan.

15.3 Media rasmi pengawal data atau pemproses data adalah termasuk saluran seperti platform media sosial, intranet, direktori telefon dan medium lain yang berkaitan.

16 Penyimpanan Rekod

16.1 Pengawal data atau pemproses data hendaklah menyimpan dan menyenggara rekod secara tepat serta betul berkenaan pegawai perlindungan data yang dilantik untuk menunjukkan pematuhan terhadap Akta 709.

MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION

GUIDELINE

APPOINTMENT OF DATA PROTECTION OFFICER

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 12A of the Personal Data Protection Act 2010 ("**Act 709**") sets the requirement for both data controller and data processor to appoint one or more data protection officer to oversee their compliance with Act 709.

1.2 This Guideline sets out the requirements to appoint data protection officer, roles and responsibilities of the data protection officer and obligations of the data controller and data processor to ensure the effective implementation of the data protection officer's role in compliance and in accordance with the Act 709.

1.3 Please note that 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. 1/2025 (Appointment of Data Protection Officer) ("**Circular No. 1/2025**"), 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 Personal Data Protection Commissioner ("**Commissioner**") pursuant to the function and responsibilities of the Commissioner under subsection 48(g) of the Act 709.

3 Interpretations

3.1 Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings as those assigned to them under the Act 709, the Circular No. 1/2025, and any other relevant legislative instruments under the Act 709.

3.2 In this Guideline, unless the context otherwise requires:

"**business contact information**"	means an individual's name, position or title, business telephone number, business address, the dedicated and official business e-mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes.

PART B: REQUIREMENTS FOR THE APPOINTMENT OF DATA PROTECTION OFFICER

4 Conditions for the Appointment of Data Protection Officer

4.1 Under the Circular No. 1/2025, the requirement for the appointment of data protection officer is subject to the conditions determined by the Commissioner.

4.2 In accordance to the section 12A of Act 709, data controller and data processor are required to appoint one or more data protection officers if their processing of personal data involves:

4.2.1 personal data exceeding 20,000 data subjects;

4.2.2 sensitive personal data including financial information data exceeding 10,000 data subjects; or

4.2.3 involves activities that require regular and systematic monitoring of personal data.

4.3 For the purposes of determining "*regular and systematic monitoring*" in paragraph 4.2.3 above, below are some examples for reference:

Examples:

- Any form of activity where data subjects are tracked and profiled online or offline for purposes of behavioural advertising will be considered as activities which require regular and systematic monitoring.

- A retail website that uses algorithms to monitor the searches and purchases of its users and based on this information, offers recommendations to them, would be carrying out "*regular and systematic monitoring*" of data subjects.

- Data controller or data processor that carry out activities such as:

  - operating a telecommunications network;

  - monitoring the wellness, fitness and health data via wearable devices; and / or

  - activities involving Close-Circuit Television (CCTV) or connected devices such as smart cars, home automation system etc.,

  would be considered as carrying out activities that may constitute "*regular and systematic monitoring*".

- The management of loyalty programme may not be considered as activities that require "*regular and systematic monitoring*" of the data subjects if the purpose of doing so was strictly to manage the data subjects' accounts and not to monitor their purchase behaviours.

4.4 Notwithstanding Para 4.2, data controller or data processor shall notify the Commissioner on the appointment of data protection officer if there is any urgency.

4.5 Data controller or data processor may keep a record on the reasons for not appointing data protection officer if they find the requirements in para 4.2 are not fulfilled.

5 Expertise and Qualifications of Data Protection Officer

5.1 Data controller or data processor must ensure that the appointed data protection officer is able to adequately carry out their tasks.

5.2 Subject to paragraphs 5.6 and 5.7 below, data controller and data processor shall determine appropriate level of qualifications, experiences, skills and expertise required for data protection officer taking into consideration:

5.2.1 the operation of personal data processing being carried out;

5.2.2 the complexity and scale of data processed;

5.2.3 the sensitivity of the personal data processed; and

5.2.4 the level of protection required for the data being processed.

5.3 The appointed data protection officer needs to possess a higher level of skill and expertise and support from the data controller or data processor depending on factors such as:

5.3.1 the scale of sensitive personal data being processed; or

5.3.2 involved in complex processing of personal data such as systematic personal data sharing between multiple organisations and cross-border personal data transfers.

Minimum Skills or Expertise

5.4 There are no minimum professional qualifications required prior to being appointed as a data protection officer, unless the data controller or data processor or the Commissioner otherwise determines from time to time.

5.5 In any event, the data controller or data processor must ensure that the appointed data protection officer can demonstrate a sound level of the following skills, qualities and expertise:

5.5.1 knowledge on the Act 709, requirement under the law data protection practices in the country (including any other applicable data protection laws, where relevant);

5.5.2 understanding of the data controller or data processor's business operations and the personal data processing operations that are carried out;

5.5.3 understanding of information technology and data security;

5.5.4 personal qualities such as integrity, understanding of corporate governance and high professional ethics;

5.5.5 ability to promote data protection culture within the organisation;

Data Protection Officer Training

5.6 In order to ensure that appointed data protection officer has the knowledge, skills and expertise required to perform his duties efficiently, the Commissioner may decide necessary or expedient mechanisms such as determining courses and training programmes including professional skills benchmarking mechanisms and other relevant programme for data protection officer.

5.7 Data controller or data processor must ensure that appointed data protection officer has sufficient training and skills to carry out duties as data protection officer efficiently by attending the relevant courses or training programmes.

6 Matters Relating to the Appointment of Data Protection Officer

6.1 The appointment of data protection officer shall not discharge data controller or data processor from the obligations to ensure compliance with the requirements of the Act 709 when processing personal data. The data controller or data processor remains responsible and liable for any non-compliance with the provisions under the Act 709.

6.2 A data protection officer may execute other official duties and responsibilities or perform additional tasks as part of his job scope, such as a legal counsel, risk management officer etc. However, the data controller or data processor shall ensure that the performance of such other tasks and functions does not cause a conflict of interest to the data protection officer.

Examples:

- A data controller or data processor's Head of Marketing is asked to carry out a marketing campaign to promote the data controller or data processor's products and accept a dual role as a data protection officer within the company. The head of marketing should not accept the role of data protection officer as the objective is to:

  (i) target as many customers as possible and process their personal data for direct marketing purposes; and

  (ii) maximise product sales, may conflict with the data protection officer's role in the organisation in ensuring compliance with the Act 709 and safeguarding customer's personal data.

- Roles such as records manager or compliance officer, are generally less likely to result in conflict of interest as these roles focus on ensuring compliance with personal data protection rights.

6.3 The data protection officer's position may be a part-time or full-time role, taking into account the organisation's function, structure and size.

6.4 In the event that an individual appointed as the data protection officer ceases their service or reaches the end of their term, the data controller or data processor shall appoint, reappoint, or hire a replacement within a reasonable time frame. The data controller and data processor shall, as soon as possible, appoint an interim data protection officer to monitor communications in the official business e-mail of the data protection officer.

Method of Appointing Data Protection Officer

6.5 Data protection officer may be appointed from among existing employees or through outsourcing services (based on a service contract signed with an individual or organisation).

6.6 Where the data protection officer is appointed through a contract, data controller or data processor is recommended to ensure that the appointment is for a term of at least two (2) years, to ensure stability.

6.7 Data controller or data processor that appoints external data protection officer must clearly, concisely and comprehensively describe the duties and obligations of the data protection officer in the service contract.

6.8 Data controller or data processor must ensure that the appointed outsource organisation designate an individual within the organisation as the lead contact and person-in-charge ("**PIC**") for liaising with the data controller or data

processor. This lead contact or PIC must be specified / referenced in the service contract with the external service provider.

Accessibility of Data Protection Officer

6.9 A data protection officer may be appointed to serve multiple data controllers or data processors, provided that the data protection officer is easily accessible by the different entities receiving the data protection officer's service.

6.10 For better responsiveness and accessibility, it is required that the data protection officer:

6.10.1 be resident in Malaysia (i.e. be physically present in Malaysia for at least 180 days in one calendar year); or

6.10.2 easily contactable via any means; and

6.10.3 be proficient in the Bahasa Melayu and English languages.

7 Notification of Data Protection Officer Appointment

7.1 Data controller that fulfills the conditions for appointing data protection officer shall register the appointed data protection officer and submit their business contact information within twenty-one (21) days from the date of appointment.

7.2 Notification to the Commissioner regarding the appointment of the data protection officer shall be submitted through the Personal Data Protection System (SPDP) via https://daftar.pdp.gov.my.

7.3 The business contact information shall be duly maintained and promptly updated by the data controller to ensure efficient communication with the data protection officer can be made at all reasonable times.

7.4 If there is a change in the appointed data protection officer or the business contact information of the data protection officer, the data controller shall promptly maintain and update the changes no later than fourteen (14) days from the effective date of the new appointment via SPDP.

PART C: THE ROLES OF DATA PROTECTION OFFICER

8 Responsibilities of Data Protection Officer in relation to the Appointing Data Controller or Data Processor

8.1 In performing his duties, data protection officer shall adopt a risk-based approach in assessing risks from the perspective of the data controller or data processor's processing operations, taking into account the nature, scope, context and purposes of the processing. He shall also coordinate and cooperate with relevant personnel of the data controller or data processor as necessary.

8.2 Data protection officer shall have at least the following core responsibilities in respect of the data processing activities of the data controller or data processor:

8.2.1 inform and provide advice to the data controller or data processor on the processing of personal data;

Examples:

- educating the data controller or data processor regarding the requirements under Act 709 applicable to its personal data processing activities.

- advising the data controller or data processor regarding different laws, regulations and related instruments, as well as industry standards and certifications for ensuring adequate compliance with personal data protection requirements.

8.2.2 support the data controller or data processor in complying with Act 709 and other related data protection laws including staying informed of data processing risks affecting the data controller or data processor;

Examples:

- collect information to identify the processing operations, activities, measures, policies or systems of the data controller or data processor and maintain a record thereof.

- advise and oversee the implementation of security measures to protect personal data from unauthorised access, disclosure, alteration or destruction, in line with both legal requirements and internal security policies.

- advise the data controller or data processor on the potential risks and impacts that may arise from the data controller or data processor's business practices.

- develop, review and/or revise the data controller or data processor's data protection policies, guidelines etc.

- consider the adoption of accreditations or certifications to demonstrate the personal data processing standards implemented by the data controller or data processor.

- advise the data controller or data processor on the necessity of executing binding agreements with third parties (e.g. data transfer agreements, sub-processing agreement etc.).

8.2.3 support the carrying out of Data Protection Impact Assessments in accordance with the requirements as may be determined by the Commissioner from time to time;

8.2.4 monitor the personal data compliance of the data controller or data processor;

Examples:

- analysing and investigating compliance of the data controller or data processor's processing activities.
- assigning and delegating responsibilities under the data controller or data processor's data protection policies to promote accountability and comprehensive supervision.
- raising awareness and training employees on the data protection requirements of the data controller or data processor.
- conducting audits on the compliance of the data controller or data processor with their data protection policies and requirements.
- issuing recommendations to close any compliance gaps that have been identified.

8.2.5 ensure proper data breach and security incident management by assisting the data controller or data processor to prepare, process and submit reports and other documents required by the Commissioner in respect of personal data breaches, within the prescribed periods; and

8.2.6 such additional responsibilities that the Commissioner or the data controller or data processor may include from time to time (e.g. as a result of technological developments).

9 Responsibilities of Data Protection Officer in relation to Data Subjects

9.1 The data protection officer shall act as a facilitator and point of contact between data subjects and the data controller or data processor regarding the processing of the data subject's personal data and their rights.

Examples:

- handle issues related to the processing of data subject's personal data (e.g. complaints).
- manage requests concerning the exercise of the data subject's rights (e.g. requests to correct and access personal data).
- educate data subjects about the processing of their personal data (e.g. informing data subjects about the purposes for processing their personal data, the third parties to whom their personal data is disclosed and their rights).
- Act as the contact point for data subjects in cases of personal data breaches and address any concerns that may arise from data subjects.

10 Responsibilities of Data Protection Officer in relation to the Commissioner

10.1 The Data Protection Officer shall act as the liaison officer and the main point of reference between the data controller or data processor and the Commissioner.

Examples:

- serves as the primary liaison officer between the data controller or data processor and the Commissioner.

- facilitate access to documents and information during inspections or investigations into the personal data processing activities of the data controller or data processor conducted by the Commissioner.

- prepare and submit information required by the Commissioner on any personal data breaches, in accordance with prescribed timelines.

- represent the data controller or data processor in industry engagement sessions or programme organised by the Commissioner.

11 Independence of Data Protection Officer

11.1 Data controller or data processor must ensure that the data protection officer is provided with the necessary resources, as outlined in paragraph 14 of these Guidelines, to enable them to perform their functions with sufficient independence and autonomy.

11.2 To safeguard the independence of the data protection officer, the data controller or data processor shall strive to avoid placing the data protection officer in a positions that could cause conflict between business interests and compliance with Act 709.

11.3 Data protection officer should have direct reporting access to senior management (or its equivalent) of the data controller or data processor.

12 Term of Service of Data Protection Officer

12.1 Data protection officer is accountable to the data controller or data processor who have appointed the data protection officer for compliance with Act 709.

12.2 Data protection officer shall not be dismissed by the data controller or data processor for performing his duties in good faith, unless the data protection officer has breached applicable laws and/or been found to have committed negligence or misconduct.

PART D: RESPONSIBILITIES OF DATA CONTROLLER AND DATA PROCESSOR

13 Involvement of Data Protection Officer

13.1 The data controller or data processor shall ensure that the data protection officer is involved in all matters related to the protection of personal data in a timely manner.

13.2 To ensure the timely involvement of the data protection officer, the data controller or data processor must engage the data protection officer in all matters related to data protection, starting from the earliest stage of the data processing lifecycle, that is from policy formulation to the collection, storage and deletion or destruction of personal data.

Examples:

- Data protection officer should be included in senior management / board meetings or relevant working groups to discuss the governance of personal data protection across the entire organisation of the data controller or data processor.

- Data protection officer must be provided with the necessary and sufficient information promptly to effectively carry out their functions.

- The views of the data protection officer should be sought as soon as the organisation's activities are reasonably considered to have implications for or

be impacted by the data processing activities of the data controller or data processor organisation.

- Data protection officer must be promptly informed and consulted in the event of a data breach or similar security incidents.

13.3 As a recommended practice, the data controller or data processor may develop data protection guidelines as an addition to the security policy, outlining scenarios in which the data protection officer's involvement is required, and disseminate these guidelines throughout the organisation.

14 Allocation of Resources to Data Protection Officer

14.1 Data controller or data processor must ensure that data protection officer is provided with adequate resources to carry out tasks effectively.

14.2 When assessing the adequacy of the resources to be provided, the data controller or data processor should consider factors such as the complexity of the data processing operations, the sensitivity of the personal data being processed and the size and structure of the organisation.

14.3 The resources that data controller or data processor may provide to support the data protection officer’s functions should be considered comprehensively.

Examples:

The following are examples of resources / support that data protection officer may receive from data controller or data processor:

- The data protection officer receives support from top management and the board of directors in carrying out his functions and responsibilities.

- The data protection officer is allocated sufficient time to perform his duties, taking into account whether his appointment is on a part-time or full-time basis, as well as whether he undertakes other tasks aside from those designated for his role.

- The data protection officer is granted access to other services such as human resources, legal, information technology, security and others to ensure they receive the necessary support, input and information from these services.

- The data protection officer is provided with adequate support in the form of financial resources, infrastructure (premises, facilities, equipment), and manpower. Depending on the size and structure of the organisation, there may be a need to establish a support team led by the data protection officer to ensure that their functions and responsibilities are carried out effectively.

- The data controller or data processor formally acknowledges the role of the data protection officer by issuing a notice to all employees within the organisation to ensure awareness and understanding of the data protection officer's existence and functions.

- The data controller or data processor provides the data protection officer with continuous recognised training in order to ensure professional development.

15 Publication and Communication of the Contact Details of Data Protection Officer

15.1 Data controller and data processor shall create a dedicated official business e-mail account for the data protection officer. This official business e-mail account must be actively monitored and maintained at all times to ensure clear, effective and seamless communication between data protection officer, Commissioner and data subjects. The dedicated official e-mail account created shall be distinct and

separate from the personal and official business work e-mail address of the individual appointed as a data protection officer.

15.2 Data controller or data processor shall publish the business contact information of the data protection officer through any or all of the following methods / channels:

15.2.1 the official website and other official media of the data controller or data processor;

15.2.2 personal data protection notices;

15.2.3 security policies and guidelines.

15.3 The official media of the data controller or data processor includes channels such as social media platforms, intranet, telephone directories, and other relevant mediums.

16 Record Keeping

16.1 Data controller or data processor shall accurately maintain and retain records of the appointed data protection officer to demonstrate compliance with the Act 709.