KEMENTERIAN DIGITAL

GARIS PANDUAN
PERLINDUNGAN DATA PERIBADI

PENILAIAN IMPAK PERLINDUNGAN DATA (DPIA)

Versi 1.0
Tarikh Terbitan: 30 April 2026

JABATAN PERLINDUNGAN DATA PERIBADI

Alamat:

JABATAN PERLINDUNGAN DATA PERIBADI
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**") memperuntukkan keperluan kepada kedua-dua pengawal data dan pemproses data untuk melantik seorang atau lebih Pegawai Perlindungan Data ("**DPO**") bagi menyelia pematuhan mereka terhadap Akta 709.

1.2 Selaras dengan Pekeliling Pesuruhjaya Perlindungan Data Bil. 1/2025 (Pelantikan Pegawai Perlindungan Data) dan Garis Panduan Pelantikan Pegawai Perlindungan Data, salah satu tanggungjawab utama DPO adalah untuk memberikan sokongan dan nasihat mengenai pelaksanaan Penilaian Impak Perlindungan Data ("**DPIA**").

1.3 Garis Panduan DPIA ("**Garis Panduan**") ini menyediakan panduan praktikal berkaitan pelaksanaan DPIA. Melalui proses ini, organisasi dapat mengenal pasti dan mengurus risiko yang berkaitan dengan aktiviti pemprosesan data peribadi secara sistematik bagi memastikan aktiviti tersebut mematuhi keperluan Akta 709.

1.4 Sila ambil perhatian bahawa contoh-contoh yang disediakan dalam Garis Panduan ini tidak bersifat menyeluruh dan hanya disertakan bagi tujuan konteks dan ilustrasi sahaja.

1.5 Garis Panduan ini melengkapi dan hendaklah dibaca bersama dengan Akta 709 dan mana-mana instrumen perundangan lain yang dikeluarkan di bawah Akta 709, sebagaimana yang mungkin dipinda dari semasa ke semasa. Garis Panduan ini tidak boleh dianggap sebagai mengatasi mana-mana undang-undang atau peraturan lain berkaitan perlindungan data peribadi yang berkuat kuasa.

2. Peruntukan Undang-Undang

2.1 Garis Panduan ini dikeluarkan oleh Pesuruhjaya Perlindungan Data ("Pesuruhjaya") selaras dengan fungsi Pesuruhjaya di bawah subseksyen 48(g) Akta 709. Selaras dengan subperenggan 5(1)(d) Pekeliling Pesuruhjaya Perlindungan Data Bil. 1/2025 (Pelantikan Pegawai Perlindungan Data), Pesuruhjaya melalui Garis Panduan ini menggariskan keperluan-keperluan berhubung dengan pelaksanaan DPIA.

3. Tafsiran

3.1 Melainkan jika ditakrifkan sebaliknya dalam Garis Panduan ini, istilah dan ungkapan yang digunakan dalam Garis Panduan ini hendaklah mempunyai makna yang sama sebagaimana yang ditetapkan di bawah Akta 709 dan mana-mana instrumen perundangan berkaitan yang dikeluarkan di bawah Akta 709.

BAHAGIAN B: PRA-DPIA

4. Apakah itu DPIA

4.1 DPIA ialah suatu penilaian impak operasi pemprosesan yang dirancang terhadap perlindungan data peribadi. Ia melibatkan aktiviti mengenal pasti, menilai dan mengurus risiko perlindungan data peribadi berdasarkan fungsi, keperluan serta proses sesebuah organisasi.

4.2 Pada dasarnya, DPIA merupakan suatu proses yang direka bentuk untuk menganalisis dan mengurangkan (mitigasi) risiko berkaitan perlindungan data peribadi.

5. Mengapa Melaksanakan DPIA

5.1 DPIA berfungsi sebagai mekanisme penting bagi membantu organisasi mengenal pasti risiko berkaitan operasi pemprosesan. Ia membolehkan organisasi menilai sama ada risiko tersebut boleh diterima setelah mengambil kira tujuan serta sifat operasi pemprosesan tersebut. Dengan mengenal pasti risiko di peringkat awal, organisasi dapat menentukan dan melaksanakan langkah rawatan risiko yang sewajarnya, termasuk tindakan pencegahan dan mitigasi. Pendekatan proaktif ini memastikan pengurusan risiko yang berkesan serta pematuhan terhadap Akta 709.

5.2 Pelaksanaan DPIA membantu organisasi memenuhi keperluan kecukupan *(adequacy)* yang wujud dalam landskap perlindungan data peribadi di peringkat antarabangsa. Sebagai contoh, Kesatuan Eropah, United Kingdom, Indonesia, Filipina dan Korea Selatan telah menjadikan DPIA sebagai satu obligasi undang-undang mandatori dalam keadaan tertentu. DPIA juga disyorkan secara nyata sebagai amalan terbaik di pelbagai bidang kuasa lain termasuk Singapura, Jepun, Australia dan New Zealand.

5.3 Pelaksanaan DPIA memperkukuh tahap akauntabiliti dan ketelusan sesebuah organisasi. Dengan membuktikan komitmen untuk melindungi data peribadi, organisasi dapat meningkatkan keyakinan dan kepercayaan orang awam terhadap aktiviti pemprosesan data.

6. Siapa Yang Bertanggungjawab Melaksanakan DPIA

6.1 Obligasi untuk melaksanakan DPIA terletak pada pengawal data. Ini adalah kerana mengikut takrifan, pemproses data tidak memproses data peribadi bagi maksudnya sendiri. Pengawal data hendaklah bertanggungjawab dalam membuat keputusan sama ada untuk meneruskan sesuatu operasi pemprosesan dan mesti memastikan semua risiko ditangani.

6.2 Walau bagaimanapun, pemproses data yang terlibat dalam operasi pemprosesan diharapkan untuk memberikan semua bantuan yang munasabah dan perlu kepada pengawal data dalam melaksanakan DPIA. Pengawal data hendaklah memperkukuhkan jangkaan ini melalui klausa kontrak yang jelas atau kaedah lain yang bersesuaian.

Kewajipan Pelaksanaan DPIA

6.3 Tanggungjawab mutlak bagi pelaksanaan DPIA dan sebarang keputusan berkaitan dengannya adalah terletak pada pengurusan kanan pengawal data.

DPO lwn Ketua Pelaksana DPIA

6.4 Salah satu tanggungjawab utama DPO adalah untuk menyokong pelaksanaan DPIA. Dalam hal ini, DPO hendaklah memberikan sokongan yang berikut:

(a) mengenalpasti sama ada DPIA perlu dilaksanakan;

(b) memberi khidmat nasihat berhubung dengan pelaksanaan DPIA serta langkah mitigasi risiko; dan

(c) membangunkan templat atau senarai semak DPIA yang disesuaikan untuk pengawal data.

6.5 DPO tidak semestinya merupakan individu yang mengetuai pelaksanaan DPIA. Ketua Pelaksana DPIA boleh terdiri daripada DPO, pengurus projek atau mana-mana kakitangan lain yang difikirkan sesuai oleh pengawal data ("**Ketua Pelaksana DPIA**").

6.6 Ketua Pelaksana DPIA merupakan kakitangan utama yang bertanggungjawab untuk merancang dan melaksanakan DPIA. Ini termasuk berunding dan mengumpul input daripada pihak berkepentingan yang berkaitan perihal operasi pemprosesan, risiko atau cabaran yang dikenal pasti, penyelesaian rawatan risiko dan langkah mitigasi yang sewajarnya untuk menangani risiko tersebut.

Penglibatan pemegang taruh

6.7 Bagi memastikan DPIA adalah komprehensif dan berkesan, ia hendaklah melibatkan semua pemegang taruh yang berkaitan daripada pelbagai fungsi dalam organisasi yang berkaitan dengan operasi pemprosesan. Ini termasuk, tetapi tidak terhad kepada:

(a) Pengurus Projek;

(b) Bahagian Teknologi Maklumat;

(c) Bahagian Undang-Undang;

(d) mana-mana pakar bidang subjek yang lain;

(e) pemproses data; dan

(f) pihak ketiga yang berkaitan seperti yang ditakrifkan di bawah Akta 709.

6.8 Semua pemegang taruh yang relevan diharapkan dapat membantu DPO serta Ketua Pelaksana DPIA dengan memberikan input yang sewajarnya dalam melengkapkan DPIA.

7. Bilakah Perlu Melaksanakan DPIA

7.1 Pengawal data hendaklah melaksanakan DPIA jika pengawal data tersebut menjangkakan bahawa sesebuah operasi pemprosesan berkemungkinan mengakibatkan risiko tinggi terhadap perlindungan data peribadi kepada subjek data.

7.2 Dalam hal ini, pengawal data dikehendaki menggunakan pendekatan dua (2) peringkat bagi menentukan tahap risiko dan menilai sama ada DPIA diperlukan:

(a) Peringkat Pertama: Pengawal data hendaklah menentukan sama ada **ambang kuantitatif** (seperti yang dijelaskan dalam perenggan 7.5) dipenuhi. Jika ambang kuantitatif dipenuhi, DPIA hendaklah dilaksanakan.

(b) Peringkat Kedua: Jika ambang kuantitatif tidak dipenuhi, DPO hendaklah melaksanakan pertimbangan terbaik dalam menilai **faktor-faktor kualitatif** (seperti yang dijelaskan dalam perenggan 7.6) untuk menentukan sama ada DPIA diperlukan.

7.3 Garis Panduan ini tidak mengurangkan keperluan yang ditetapkan di bawah mana-mana instrumen undang-undang atau pengawalseliaan berkenaan keadaan di mana DPIA perlu dilaksanakan. Sekiranya terdapat obligasi yang mengatasi instrumen-instrumen tersebut, keperluan yang lebih luas hendaklah terpakai.

7.4 Dalam sebarang situasi di mana keperluan untuk melaksanakan DPIA tidak jelas, adalah wajar bagi pengawal data untuk melaksanakan DPIA sebagai amalan terbaik, memandangkan DPIA merupakan alat yang berguna untuk membina kepercayaan dengan subjek data, mengurus risiko perlindungan data peribadi dan memudahkan pematuhan terhadap Akta 709.

Ambang Kuantitatif

7.5 Situasi pemprosesan berikut dianggap berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data peribadi kepada subjek data, sekali gus mencetuskan keperluan pelaksanaan DPIA:

(a) pemprosesan data peribadi yang dijangka melibatkan lebih daripada 20,000 subjek data; atau

(b) pemprosesan data peribadi sensitif, termasuk data maklumat kewangan, yang dijangka melibatkan lebih daripada 10,000 subjek data.

(secara kolektif, "**Ambang Kuantitatif**").

Faktor-faktor Kualitatif

7.6 Jika pemprosesan tersebut tidak memenuhi mana-mana Ambang Kuantitatif, DPO hendaklah menggunakan pertimbangan terbaik dalam menilai faktor kualitatif lain yang berkemungkinan mengakibatkan risiko tinggi terhadap perlindungan data peribadi subjek data, sehingga memerlukan pelaksanaan DPIA. Adalah ditegaskan bahawa faktor kualitatif ini adalah tidak menyeluruh mahupun ekslusif dan dan termasuk tetapi tidak terhad kepada perkara berikut:

(a) Potensi kesan undang-undang atau kesan signifikan terhadap subjek data (contoh: impak yang ketara terhadap status atau hak undang-undang, status kewangan, kesihatan, reputasi, akses kepada perkhidmatan atau peluang ekonomi atau sosial subjek data);

Contoh:

(1) Contoh 1: Pemprosesan data peribadi sensitif yang boleh memberi kesan signifikan kepada akses insurans subjek data

Situasi: Sebuah syarikat insurans mengumpul dan memproses maklumat kesihatan seperti sejarah perubatan atau data yang diperoleh daripada aplikasi penjejakan kecergasan bagi menentukan kelayakan insurans subjek data, menetapkan kadar premium atau meluluskan perlindungan.

Mengapa DPIA diperlukan: Pengawal data hendaklah melaksanakan DPIA kerana pemprosesan tersebut melibatkan data peribadi sensitif dan pembuatan keputusan secara automatik yang memberi kesan signifikan kepada akses subjek data terhadap perlindungan insurans.

(2) Contoh 2: Pemprosesan data kewangan peribadi yang mungkin menjejaskan akses subjek data kepada kemudahan pinjaman secara signifikan

Situasi: Sebuah institusi kewangan menggunakan sistem pemarkahan kredit automatik untuk menilai permohonan pinjaman atau kredit. Sistem tersebut meluluskan atau menolak permohonan secara automatik tanpa semakan manusia, yang mengakibatkan impak serta merta terhadap skor kredit, kedudukan kewangan dan akses subjek data kepada perkhidmatan kewangan.

Mengapa DPIA diperlukan: Pemprosesan tersebut melibatkan pembuatan keputusan secara automatik berdasarkan data peribadi dan kewangan, yang mungkin memberi kesan langsung dan signifikan kepada hak dan peluang ekonomi subjek data. Oleh itu, pengawal data hendaklah melaksanakan DPIA.

(b) pemantauan sistematik terhadap subjek data;

Contoh:

(1) Contoh 1: Pemantauan sistematik terhadap individu dalam tetapan komersial

Situasi: Sebuah rantaian peruncitan menggunakan teknologi pengecaman wajah di kesemua kedainya untuk mengenal pasti pelanggan berulang yang berdaftar dalam program kesetiaannya. Apabila subjek data memasuki sebuah kedai, sistem tersebut, secara automatik memadankan imej wajah subjek data dengan rekod yang disimpan untuk menyediakan diskaun diperibadikan berdasarkan sejarah pembelian.

Mengapa DPIA diperlukan: Walaupun tujuan pemprosesan adalah untuk meningkatkan pengalaman pelanggan dan kecekapan pemasaran, pemprosesan ini melibatkan pemantauan sistematik terhadap subjek data dalam persekitaran komersial dan penggunaan data biometrik (ciri wajah) untuk pengecaman. Pemprosesan sedemikian berkemungkinan menimbulkan risiko tinggi seperti salah pengecaman, pemprofilan atau pencerobohan privasi subjek data. Oleh itu, sebelum pelaksanaan teknologi pengecaman wajah, pengawal data hendaklah melaksanakan DPIA.

(2) **Contoh 2: Penjejakan berterusan terhadap lokasi dan tingkah laku subjek data berhubung dengan transaksi komersial**

Situasi: Sebuah syarikat penghantaran makanan menawarkan satu ciri kesetiaan dalam aplikasi yang menjejaki data geolokasi subjek data apabila aplikasi dibuka atau pesanan dibuat. Sistem tersebut merekodkan alamat penghantaran, penjual makanan yang kerap dikunjungi, tempoh masa yang diluangkan dalam aplikasi dan tingkah laku melayari aplikasi. Sistem ini memadankan maklumat tersebut dengan rekod pembelian terdahulu bagi mengenal pasti pola tingkah laku seperti tabiat berbelanja, waktu makan dan

penjualan makanan pilihan. Syarikat menggunakan dapatan ini untuk menyampaikan iklan bersasar dan promosi berdasarkan lokasi, sekaligus mempengaruhi keputusan pembelian dan hasil pemasaran subjek data.

Mengapa DPIA diperlukan: Pemprosesan tersebut melibatkan penjejakan berterusan terhadap lokasi dan tingkah laku subjek data yang berkaitan dengan transaksi komersial. Aktiviti pemantauan sistematik dan pemprofilan sedemikian berkemungkinan mendatangkan risiko yang tinggi terhadap perlindungan data peribadi. Oleh itu, pengawal data hendaklah melaksanakan DPIA.

(c) penggunaan teknologi inovatif, iaitu teknologi yang melibatkan produk (barangan atau perkhidmatan) baharu atau ditambah baik secara signifikan, proses baharu, kaedah pemasaran baharu, kaedah organisasi baharu dalam amalan perniagaan atau organisasi tempat kerja atau hubungan luar yang baharu;

Contoh:

(1) Contoh 1: Penambahbaikan Proses Perniagaan melalui Teknologi Inovatif

Situasi: Sebuah institusi kewangan mengendalikan aplikasi perbankan mudah alih yang membolehkan pelanggan melakukan transaksi komersial seperti pindahan dana, bayaran bil dan pembelian dalam talian menggunakan pengesahan biometrik cap jari. Pengawal data kemudiannya memutuskan untuk menambah baik proses ini dengan menyepadukan ciri-ciri pengesahan biometrik berpacukan Kecerdasan Buatan (AI) seperti pengecaman wajah untuk memberikan lapisan keselamatan tambahan.

Mengapa DPIA diperlukan: Pemprosesan ini melibatkan penggunaan teknologi yang baharu kepada organisasi. Perubahan ini berkemungkinan menimbulkan risiko yang signifikan terhadap privasi subjek data. Peralihan kepada pengecaman wajah meningkatkan jumlah dan kerumitan data peribadi sensitif yang diproses. Oleh yang demikian, pengawal data hendaklah melaksanakan DPIA.

(2) Contoh 2: Teknologi Inovatif dalam Amalan di Tempat Kerja

Situasi: Sebuah organisasi pada masa ini menggunakan kaedah manual untuk memantau prestasi pekerja. Pengawal data telah memutuskan untuk mengguna pakai sistem Kecerdasan Buatan (AI) bagi mengautomasikan pemantauan

prestasi. Sistem AI tersebut menjana skor prestasi dan ringkasan tingkah laku, yang kemudiannya digunakan sebagai asas utama bagi keputusan berkaitan kenaikan pangkat, ganjaran atau tindakan tatatertib.

Mengapa DPIA diperlukan: Pemprosesan ini melibatkan pelaksanaan teknologi yang baharu dalam persekitaran operasi organisasi. Peralihan kepada pemantauan automatik berkemungkinan memberi kesan yang signifikan kepada hak pekerjaan, reputasi profesional dan privasi subjek data. Oleh yang demikian, pengawal data hendaklah melaksanakan DPIA.

(d) penafian atau sekatan terhadap hak subjek data;

Contoh:

(1) Contoh 1: Penafian atau sekatan akses kepada perkhidmatan

Situasi: Sebuah penyedia perkhidmatan e-panggilan mewajibkan subjek data untuk memberikan persetujuan bagi penjejakan tingkah laku yang berterusan seperti pemantauan lokasi masa nyata, corak perjalanan dan interaksi dalam aplikasi, sebagai syarat mandatori untuk mengakses perkhidmatannya. Subjek data yang enggan memberikan persetujuan mungkin dinafikan akses kepada perkhidmatan tersebut sepenuhnya (sebagai contoh, tidak dapat menempah perjalanan) atau mungkin menghadapi sekatan tertentu (seperti tidak layak untuk mendapat diskaun atau tawaran promosi).

Mengapa DPIA diperlukan: Amalan ini melibatkan penafian atau sekatan terhadap hak subjek data, terutamanya kebebasan untuk menahan atau menarik balik persetujuan tanpa sebarang kerugian. Oleh yang demikian, pengawal data hendaklah melaksanakan DPIA.

(2) Contoh 2: Sekatan sistematik daripada melaksanakan hak akses

Situasi: Sebuah syarikat e-dagang membolehkan subjek data membuat pembelian melalui aplikasi mudah alihnya. Walau bagaimanapun, apabila subjek data meminta akses kepada data peribadinya, seperti sejarah pembelian atau butiran akaun, aplikasi tersebut tidak menyediakan mekanisme langsung untuk mengemukakan permintaan tersebut. Sebaliknya, subjek data diarahkan ke alamat e-mel luaran atau nombor telefon untuk menyerahkan permintaan itu.

Mengapa DPIA diperlukan: Amalan ini mewujudkan halangan pentadbiran yang menghalang subjek data daripada melaksanakan haknya untuk mengakses data peribadi. Memandangkan ini melibatkan sekatan sistemik terhadap hak subjek data, pengawal data hendaklah melaksanakan DPIA.

(e) penjejakan lokasi atau tingkah laku subjek data;

Contoh:

(1) Contoh 1: Penjejakan berterusan melalui aplikasi runcit

Situasi: Sebuah syarikat peruncitan menggunakan aplikasi mudah alih untuk menjejak lokasi geografi subjek data secara berterusan, laluan pergerakan dalam kedai dan tempoh masa di ruangan tertentu. Data peribadi tersebut digunakan untuk menganalisis tingkah laku subjek data, mengoptimumkan susun atur kedai dan menyampaikan iklan bersasar atau promosi berdasarkan pola pergerakan masa nyata.

Mengapa DPIA diperlukan: Memandangkan pemprosesan ini melibatkan penjejakan yang berkala dan sistematik terhadap lokasi serta tingkah laku subjek data, pengawal data hendaklah melaksanakan DPIA.

(2) Contoh 2: Analitik laluan-klik dalam talian (*Online Click-path Analytics*)

Situasi: Sebuah platform e-dagang menjejak tingkah laku dalam talian subjek data seperti sejarah pelayaran, klik, masa yang diluangkan pada halaman dan aktiviti pembelian bagi meramal niat pembelian, memperibadikan harga jualan serta menyampaikan iklan bersasar.

Mengapa DPIA diperlukan: Pemprosesan ini melibatkan pemantauan tingkah laku subjek data secara sistematik dan berterusan untuk tujuan komersial dan pemprofilan. Pemprosesan ini berkemungkinan memberi kesan signifikan terhadap hak subjek data. Oleh itu, pengawal data hendaklah melaksanakan DPIA.

(f) penyasaran terhadap kanak-kanak atau individu rentan; dan

Contoh:

Pemprosesan data peribadi kanak-kanak bagi tujuan pengiklanan

Situasi: Sebuah institusi pendidikan melalui platform teknologinya, mengumpul data peribadi kanak-kanak dan berniat untuk menyiarkan iklan di dalam platform tersebut.

Mengapa DPIA diperlukan: Pemprosesan ini melibatkan data peribadi kanak-kanak dan aktiviti pemprofilan, terutamanya bagi tujuan pengiklanan. Ini menimbulkan risiko terhadap perlindungan hak kanak-kanak dan potensi penyasaran komersial terhadap golongan bawah umur. Oleh yang demikian, pengawal data hendaklah melaksanakan DPIA.

(g) pembuatan keputusan secara automatik dan pemprofilan yang menimbulkan risiko yang tinggi terhadap subjek data.

(secara kolektif, "**Faktor-Faktor Kualitatif**").

7.7 DPO hendaklah menggunakan pertimbangan yang terbaik dalam menilai faktor-faktor kualitatif, yang mungkin termasuk faktor yang tidak dinyatakan secara nyata di atas, bagi menentukan sama ada suatu operasi pemprosesan berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data peribadi kepada subjek data.

Illustrasi: Menentukan Keperluan untuk Melaksanakan DPIA

(i) Sebuah organisasi berhasrat untuk menyimpan data peribadi pelanggannya dengan penyedia perkhidmatan awan *(cloud service provider)* luar. Cadangan penyimpanan sedemikian merupakan suatu operasi pemprosesan.

Ambang Kuantitatif

(ii) Pengawal data sesebuah organisasi, dengan berunding bersama DPO, hendaklah terlebih dahulu mempertimbangkan sama ada operasi pemprosesan memenuhi Ambang Kuantitatif (iaitu sama ada pemprosesan berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data peribadi subjek data), dengan mengemukakan soalan berikut:

a) Adakah operasi pemprosesan tersebut dijangka melibatkan lebih daripada 20,000 subjek data?

b) Adakah operasi pemprosesan data peribadi sensitif tersebut termasuk maklumat kewangan, dijangka melibatkan lebih daripada 10,000 subjek data?

Jika mana-mana jawapan di atas adalah '**Ya**', Ketua Pelaksana DPIA hendaklah melaksanakan DPIA terhadap operasi pemprosesan tersebut.

(iii) Jika **kedua-dua** jawapan di atas adalah '**Tidak**', DPO setelah berunding dengan Ketua Pelaksana DPIA, hendaklah melaksanakan pertimbangan terbaik dalam menilai **Faktor-Faktor Kualitatif** bagi menentukan sama ada operasi pemprosesan berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data peribadi kepada subjek data.

Faktor-Faktor Kualitatif

(iv) Faktor-faktor Kualitatif yang relevan mungkin termasuk, sebagai contoh:

a) jenis data peribadi yang terlibat (contoh: sama ada pemprosesan tersebut berpotensi membawa kesan undang-undang atau kesan signifikan terhadap subjek data); dan

b) lokasi penyedia perkhidmatan awan (contoh: jika penyedia perkhidmatan terletak di luar Malaysia, sama ada tempat tersebut mempunyai undang-undang perlindungan data yang setara dengan Akta 709 bagi melindungi data peribadi).

(v) Jika pada pertimbangan terbaik DPO, operasi pemprosesan tersebut berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data peribadi kepada subjek data, Ketua Pelaksana DPIA hendaklah melaksanakan DPIA.

(vi) Jika DPO berpendapat bahawa operasi pemprosesan tersebut tidak berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data

peribadi kepada subjek data, DPO boleh memberi nasihat agar DPIA dilaksanakan sebagai suatu amalan terbaik.

BAHAGIAN C: PELAKSANAAN DPIA

8. Cara Melaksanakan DPIA

8.1 Pengawal data diharapkan untuk menerima pakai pendekatan lima langkah iaitu Perihal *(Describe)*, Nilai *(Evaluate)*, Kenal pasti *(Identify)*, Pertimbang *(Consider)* dan Taksir *(Assess)* atau lebih dikenali dengan singkatannya DEICA ("DEICA"), bagi menganalisis sesuatu operasi pemprosesan berkaitan dengan tujuan, risiko spesifik dan langkah-langkah yang akan diambil:

(a) **Langkah 1: *Describe*** – Perihalkan operasi pemprosesan (termasuk takat penglibatan data peribadi dan aliran data) serta tujuan pemprosesan tersebut;

Penerangan:

Langkah ini melibatkan penjelasan mengenai pemprosesan berdasarkan aspek-aspek berikut:

(i) **Sifat:** Apa yang dirancang terhadap data peribadi. (Contoh: bagaimana data peribadi akan dikumpul, disimpan, digunakan, diakses dan dizahirkan kepada pihak-pihak yang berkaitan);

(ii) **Skop:** Apa yang dirangkumi oleh pemprosesan. (Contoh: jumlah dan kepelbagaian data peribadi, takat, kekerapan dan tempoh pemprosesan, bilangan subjek data yang terlibat, kawasan geografi yang diliputi serta sama ada terdapat pemindahan rentas sempadan);

(iii) **Konteks:** Gambaran yang lebih luas yang mungkin menjejaskan jangkaan dan impak. (Contoh: sifat hubungan organisasi dengan subjek data dan sebarang isu awam semasa yang menjadi kepentingan awam); dan

(iv) **Tujuan:** Sebab organisasi ingin memproses data peribadi yang mungkin merangkumi hasil yang disasarkan untuk subjek data serta manfaat yang dijangkakan bagi organisasi tersebut.

(b) **Langkah 2: *Evaluate*** – Nilai pematuhan, keperluan dan kekadaran (*proportionality*) operasi pemprosesan berhubung dengan maksud pemprosesannya;

Penerangan

Langkah ini melibatkan pertimbangan terhadap:

(i) sama ada perancangan organisasi benar-benar membantu mencapai maksud yang diniatkan; dan

(ii) sama ada terdapat cara lain yang munasabah untuk mencapai hasil yang sama tanpa melibatkan pemprosesan yang dicadangkan atau dengan takat pemprosesan yang lebih terhad (contoh: menentukan sama ada pemindahan rentas sempadan benar-benar diperlukan dalam operasi pemprosesan bagi mencapai maksud yang diniatkan).

(c) **Langkah 3: *Identify*** – Kenal pasti dan analisis risiko spesifik terhadap perlindungan data peribadi subjek data;

Penerangan:

Langkah ini melibatkan pertimbangan terhadap risiko pelanggaran mana-mana Prinsip-Prinsip Perlindungan Data Peribadi atau keperluan lain di bawah **Akta 709**, serta potensi impak terhadap subjek data dan sebarang kemudaratan yang mungkin disebabkan oleh pemprosesan tersebut, contohnya:

(i) risiko keselamatan (termasuk punca risiko dan potensi impak bagi setiap jenis pelanggaran);
(ii) ketidakupayaan untuk melaksanakan hak subjek data;
(iii) kehilangan kawalan terhadap penggunaan data peribadi;
(iv) kecurian identiti atau penipuan;
(v) kerugian kewangan;
(vi) kecederaan fizikal;
(vii) kehilangan kerahsiaan; dan
(viii) undang-undang privasi dan perlindungan data yang tidak mencukupi di negara di mana data peribadi tersebut dipindahkan.

Analisis risiko spesifik yang dikenal pasti hendaklah mempertimbangkan kedua-dua aspek **Kebarangkalian (*Likelihood*)** dan **Impak *(Impact)*** daripada kemudaratan yang mungkin berlaku. Sebuah Matriks Risiko 3 x 3 (seperti di bawah) digunakan untuk menentukan tahap risiko bagi setiap risiko spesifik. Skor risiko diperoleh dengan mendarabkan skor Kebarangkalian dengan skor Impak.

1. Matriks Risiko (3 x 3)

Jadual di bawah merupakan contoh Matriks Risiko 3 x 3 bagi pengiraan tahap risiko. Risiko bagi setiap kemudaratan dikira dengan mendarabkan Kebarangkalian dengan Impak daripada kemudaratan yang mungkin berlaku.

Matriks Risiko		**Kebarangkalian**		
		Rendah (1)	**Sederhana (2)**	**Tinggi (3)**
Impak	**Tinggi (3)**	Sederhana (3)	Tinggi (6)	Tinggi (9)
	Sederhana (2)	Rendah (2)	Sederhana (4)	Tinggi (6)
	Rendah (1)	Rendah (1)	Rendah (2)	Sederhana (3)

2. Takrifan Kriteria

a) Kebarangkalian (*Likelihood*)

Kebarangkalian (*Likelihood*) menilai probabiliti atau peluang berlakunya sesuatu peristiwa risiko (contoh: pelanggaran data, penzahiran secara tidak sengaja, akses tanpa kebenaran atau kehilangan data peribadi) dalam tempoh masa atau konteks operasi tertentu.

Kebarangkalian	**Kriteria**
Rendah (1)	Peristiwa tidak mungkin berlaku atau mempunyai peluang yang amat tipis untuk berlaku. Kawalan atau sistem sedia ada telah

	dilaksanakan dan memadai untuk melindungi subjek data.
Sederhana (2)	Peristiwa berkemungkinan berlaku atau diketahui pernah berlaku dalam industri tertentu. Kawalan atau sistem sedia ada telah dilaksanakan tetapi mungkin mempunyai had atau kelemahan.
Tinggi (3)	Peristiwa sangat mungkin berlaku atau pernah berlaku sebelum ini. Kawalan atau sistem mempunyai had atau kelemahan serta mempunyai kerentanan yang signifikan.

b) Impak

Impak merujuk kepada tahap keseriusan potensi kemudaratan terhadap subjek data sekiranya risiko tersebut menjadi kenyataan. Ia memberi tumpuan kepada sama ada pemprosesan tersebut berkemungkinan mengakibatkan risiko tinggi terhadap perlindungan data peribadi bagi subjek data tersebut.

Impak	**Kriteria**
Rendah (1)	Tidak mungkin mengakibatkan risiko material. Data yang terlibat tidak sensitif dan sebarang pelanggaran hanya akan mengakibatkan kesulitan yang minimum tanpa impak signifikan terhadap hak atau kepentingan subjek data.
Sederhana (2)	Berkemungkinan mengakibatkan risiko. Pemprosesan tersebut boleh menyebabkan kemudaratan material tetapi bukan jenis yang kekal (tidak boleh diubah), seperti perasaan malu, kerugian kewangan kecil, tekanan emosi atau kehilangan kawalan data yang terhad.

Tinggi (3)	Berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data peribadi bagi subjek data. Kemudaratan mungkin signifikan atau bersifat kekal, termasuk kerugian kewangan yang besar, kecurian identiti, diskriminasi atau kerosakan reputasi yang teruk.

3. Respons Risiko dan Rawatan Risiko

Skor Risiko	Tahap	Tindakan Yang Diperlukan
1-2	**Rendah**	**Pemantauan –** Risiko adalah terkawal. Pemantauan diteruskan melalui kawalan sedia ada dan prosedur operasi standard.
3-4	**Sederhana**	**Mitigasi –** Memperkukuh langkah-langkah mitigasi. Melaksanakan kawalan teknikal dan/atau organisasi tambahan untuk mengurangkan kebarangkalian atau impak risiko.
6-9	**Tinggi**	**Tindakan Mandatori –** Berkemungkinan mengakibatkan risiko yang tinggi kepada subjek data. DPIA adalah perlu. Langkah-langkah rawatan risiko yang kukuh hendaklah dilaksanakan.

<u>Ilustrasi: Penilaian Risiko bagi Kecurian Identiti</u>

Contoh berikut menunjukkan bagaimana suatu risiko spesifik dikenal pasti dan dianalisis.

Sebagai ilustrasi, jika sesebuah operasi pemprosesan menimbulkan risiko spesifik kecurian identiti, pengawal data hendaklah mempertimbangkan:

(i) **Kebarangkalian** (contohnya, sama ada kecurian identiti pernah berlaku sebelum ini dalam organisasi, dalam kalangan pesaing dalam industri yang sama atau dalam operasi pemprosesan yang serupa);

(ii) **Impak** (contoh: mengambil kira tahap kemudaratan yang mungkin berlaku, berdasarkan jenis data peribadi yang terlibat seperti nombor akaun bank dan profil subjek data);

(iii) **Menentukan tahap risiko** (contoh: jika risiko spesifik kecurian identiti dinilai sebagai "Sederhana" bagi kebarangkalian dan "Tinggi" bagi keseriusan impak, risiko tersebut akan dianggap sebagai "Risiko Tinggi".

Dalam keadaan sedemikian, langkah-langkah mitigasi yang lebih kukuh hendaklah dilaksanakan dalam Langkah 4 (Pertimbang), yang mana kemudiannya mungkin mempengaruhi baki tahap risiko keseluruhan dalam Langkah 5 (Nilai).

(d) **Langkah 4: *Consider*** – Pertimbang langkah-langkah yang perlu diambil untuk menangani risiko spesifik yang dikenal pasti bagi menjamin perlindungan data peribadi; dan

Penerangan:

Langkah ini mungkin melibatkan mana-mana perkara berikut:

(i) tidak mengumpul jenis data tertentu;

(ii) mengurangkan kekerapan pemprosesan atau memendekkan tempoh penyimpanan;

(iii) melaksanakan langkah-langkah keselamatan tambahan;

(iv) menyahnama *(anonymise)* atau menyamarkan *(pseudonymise)* data peribadi tertentu;

(v) menggunakan teknologi yang berbeza;

(vi) memasukkan perlindungan kontraktual tambahan dengan pihak ketiga yang terlibat dalam pemprosesan; dan

(vii) menjalankan Penilaian Impak Pemindahan (TIA) untuk menentukan sama ada pemindahan tersebut dibenarkan di bawah Akta 709 dan/atau negara penerima mempunyai undang-undang perlindungan data dan privasi yang mencukupi.

(e) **Langkah 5: *Assess*** – Taksir baki tahap risiko keseluruhan (contoh: tinggi, sederhana, rendah) bagi operasi pemprosesan tersebut.

Penerangan:

Langkah ini mungkin melibatkan pertimbangan terhadap tahap risiko yang ditetapkan bagi setiap risiko spesifik yang dikenal pasti dan langkah-langkah yang dicadangkan untuk menangani risiko spesifik tersebut, bagi menentukan baki tahap risiko keseluruhan.

8.2 Bagi menggambarkan bagaimana prosedur DEICA boleh diguna pakai, satu (1) Templat DPIA disediakan di **Lampiran A** sebagai rujukan. Templat DPIA yang dicadangkan ini bertujuan sebagai panduan dan penggunaan kandungannya adalah mengikut budi bicara organisasi. Pengawal data boleh menyesuaikan Templat ini mengikut keperluan atau keadaan khusus, membangunkan templat tersendiri (yang disesuaikan daripada Templat ini) atau membangunkan sebarang senarai semak tambahan, selagi ia selaras dengan Garis Panduan ini.

BAHAGIAN D: PASCA-DPIA

9. Laporan kepada Pengurusan Kanan

9.1 Setelah DPIA selesai dilaksanakan, sekiranya baki tahap risiko keseluruhan dinilai sebagai "Tinggi", hasil dapatan tersebut hendaklah dilaporkan kepada pengurusan kanan organisasi. Melainkan ditentukan sebaliknya oleh organisasi, semua risiko, tanpa mengira tahapnya hendaklah juga dilaporkan kepada pengurusan kanan bagi memastikan pihak pengurusan sentiasa dimaklumkan sepenuhnya mengenai semua risiko yang dikenal pasti.

9.2 Pengurusan kanan hendaklah mempertimbangkan hasil dapatan DPIA dan memberi input berkenaan operasi pemprosesan. Input tersebut mungkin melibatkan:

(a) menerima baki tahap risiko keseluruhan yang timbul daripada operasi pemprosesan;

(b) memutuskan sebarang langkah mitigasi tambahan bagi menguruskan risiko tersebut; dan

(c) memperuntukkan sumber yang sewajarnya bagi melaksanakan langkah-langkah mitigasi risiko.

10. Pelaksanaan Langkah Mitigasi Risiko

10.1 Setelah keputusan dibuat untuk meneruskan operasi pemprosesan, langkah-langkah mitigasi risiko yang dikenal pasti hendaklah dilaksanakan dengan sewajarnya bagi menangani dan mengurus risiko spesifik yang dikenal pasti dalam DPIA.

10.2 Ketua Pelaksana DPIA merupakan kakitangan utama yang bertanggungjawab untuk menyelia pelaksanaan langkah-langkah mitigasi risiko. DPO hendaklah memberikan sokongan dan nasihat mengenai pelaksanaan tersebut selaras dengan dasar perlindungan data organisasi, amalan terbaik industri dan Akta 709. Walau bagaimanapun, tanggungjawab mutlak untuk melaksanakan langkah-langkah mitigasi risiko tersebut terletak pada pengurusan kanan pengawal data.

11. Penerbitan, Kesahan dan Pemantauan

11.1 Bagi menggalakkan ketelusan dan kebertanggungjawaban, pengawal data boleh mempertimbangkan untuk menerbitkan DPIA bagi meningkatkan kepercayaan terhadap aktiviti pemprosesan data peribadinya. Bagi melindungi maklumat sensitif komersial atau mengurus risiko keselamatan yang lain (termasuk yang melibatkan data peribadi), DPIA yang diterbitkan boleh disunting. Sebagai alternatif, ringkasan DPIA boleh diterbitkan.

11.2 DPIA yang siap adalah **sah bagi tempoh dua (2) tahun** dari tarikh penyiapan. Setelah **tamat tempoh** tersebut, **DPIA baharu** hendaklah dilaksanakan.

11.3 Dalam apa jua keadaan, DPIA bukanlah suatu aktiviti sekali sahaja tetapi memerlukan pemantauan berterusan dan semakan berkala. Walau apa pun tempoh sah laku tersebut dan sepanjang tempoh operasi pemprosesan, Ketua Pelaksana DPIA hendaklah memantau sebarang perkembangan yang boleh menjejaskan operasi pemprosesan, risiko yang dikenal

pasti dan langkah-langkah mitigasi risiko yang diguna pakai (contoh: perubahan pada tujuan pemprosesan atau kerentanan baharu yang dikenal pasti dalam teknologi yang digunakan). Ketua Pelaksana DPIA hendaklah menangani perkembangan tersebut dengan sewajarnya bagi memastikan perlindungan berterusan terhadap subjek data.

12. Penyimpanan Rekod

12.1 Dalam apa jua keadaan, DPIA yang dilaksanakan serta semua dokumentasi yang berkaitan hendaklah diselenggara dengan sewajarnya untuk tempoh sekurang-kurangnya dua (2) tahun dari penamatan operasi pemprosesan. Sebagai contoh, jika operasi pemprosesan berlangsung selama lima (5) tahun, DPIA dan rekod yang berkaitan hendaklah disimpan untuk dua (2) tahun selepas operasi tersebut dihentikan. Oleh yang demikian, tempoh penyimpanan rekod secara keseluruhannya adalah sekurang-kurangnya tujuh (7) tahun.

12.2 Rekod tersebut hendaklah dikemukakan untuk pemeriksaan atas permintaan Pesuruhjaya.

LAMPIRAN A: TEMPLAT DPIA

Bil.	Soalan	Respons	Nota Panduan
<u>Pra-DPIA</u>: Menentukan sama ada DPIA diperlukan			
Pemprosesan Dirancang			
1.	Apakah maksud dan operasi pemprosesan data peribadi yang dirancang?	*Sila berikan penjelasan ringkas* ("**Pemprosesan Dirancang**")	<u>Contoh respons</u>: *Melantik penyedia perkhidmatan sumber manusia, Z, untuk menganalisis maklum balas tinjauan pelanggan dan menyimpan data peribadi mereka di Singapura.*
Penentu			
2.	Adakah **Pemprosesan Dirancang** tersebut melibatkan data peribadi yang dijangka melebihi 20,000 subjek data?	☐ Ya ☐ Tidak Penjelasan: *Sila berikan*	Sila tandakan kotak pilihan yang berkenaan bagi setiap soalan. <u>Contoh respons bagi penjelasan</u>: i. Pemprosesan Dirancang melibatkan pemprosesan data peribadi melebihi 20,000 subjek data; atau ii. Pemprosesan Dirancang melibatkan pemprosesan data peribadi sensitif termasuk maklumat kewangan, yang melebihi 10,000 subjek data.
3.	Adakah **Pemprosesan Dirancang** tersebut melibatkan data peribadi sensitif termasuk maklumat kewangan yang dijangka melebihi 10,000 subjek data?	☐ Ya ☐ Tidak Penjelasan: *Sila berikan*	

Bil.	Soalan	Respons	Nota Panduan
4.	Adakah Pemprosesan Dirancang melibatkan mana-mana **Faktor Kualitatif** yang berkemungkinan mengakibatkan risiko yang tinggi terhadap perlindungan data peribadi subjek data sehingga pada pertimbangan DPO, **DPIA hendaklah dilaksanakan untuk penilaian lanjut terhadap risiko-risiko tersebut?**	☐ Potensi kesan undang-undang atau kesan signifikan terhadap subjek data ☐ Pemantauan sistematik terhadap subjek data ☐ Penggunaan teknologi inovatif ☐ Penafian atau sekatan terhadap hak subjek data ☐ Penjejakan lokasi atau tingkah laku subjek data ☐ Penyasaran terhadap kanak-kanak atau individu rentan ☐ Pembuatan keputusan secara automatik dan pemprofilan yang menimbulkan risiko yang tinggi terhadap subjek data ☐ Faktor lain yang memerlukan pelaksanaan DPIA: *Sila huraikan* ☐ Tidak berkenaan.	Sila tandakan semua kotak pilihan yang berkenaan. <u>Contoh</u>: (i) Potensi kesan undang-undang atau kesan signifikan terhadap subjek data *(contoh: impak yang ketara terhadap status atau hak undang-undang, status kewangan, kesihatan, reputasi, akses kepada perkhidmatan atau peluang ekonomi atau sosial subjek data);* (ii) Pemantauan sistematik terhadap subjek data *(contoh: pemantauan sistematik terhadap individu dalam tetapan komersial);* (iii) Penggunaan teknologi inovatif *(contoh: proses perniagaan yang ditambah baik secara signifikan melalui teknologi inovatif*); (iv) Penafian atau sekatan terhadap hak subjek data *(contoh: sekatan sistematik terhadap hak untuk mengakses);* (v) Penjejakan lokasi atau tingkah laku subjek data *(contoh: analitik laluan-klik (click-path analytics) dalam talian);* (vi) Penyasaran terhadap kanak-kanak atau individu-rentan *(contoh: memproses data peribadi kanak-kanak*

Bil.	Soalan	Respons	Nota Panduan
			bagi tujuan menawarkan perkhidmatan kepada mereka); (vii) Pembuatan keputusan secara automatik dan pemprofilan yang menimbulkan risiko yang tinggi terhadap subjek data; (viii) Mana-mana faktor lain yang memerlukan pelaksanaan DPIA *(contoh: risiko kecederaan fizikal sekiranya berlaku pelanggaran data).*
Hasil Dapatan			
5.	Adakah **Pemprosesan Dirancang** memerlukan DPIA?	☐ Ya ☐ Tidak	Sila tandakan "Tidak", jika: (i) soalan 2 dan 3 dijawab "Tidak"; **DAN** (ii) soalan 4 dijawab "Tidak berkenaan". Jika tidak, sila tandakan "Ya" dan teruskan untuk menjawab soalan-soalan di bawah.
DPIA: Melaksanakan lima (5) langkah di bawah DEICA			
D – Perihalan Pemprosesan Dirancang			
6.	Apakah **sifat Pemprosesan Dirancang**?	*Sila terangkan*	Ilustrasi dan contoh: Penerangan hendaklah merangkumi apa yang dirancang untuk dilakukan terhadap data peribadi: (i) Bagaimana data akan dikumpul;

Bil.	Soalan	Respons	Nota Panduan
			(ii) Bagaimana data akan disimpan; (iii) Bagaimana data akan digunakan; (iv) Siapa yang akan mempunyai akses kepada data; (v) Kepada siapa data tersebut akan dizahirkan; (vi) Sama ada sebarang pemproses data akan dilantik; (vii) Tempoh penyimpanan yang berkenaan; (viii) Langkah-langkah keselamatan yang akan dilaksanakan.
7.	Apakah **skop Pemprosesan Dirancang**?	*Sila terangkan*	Ilustrasi dan contoh: Perincian hendaklah menjelaskan skop pemprosesan, sebagai contoh: (i) Jumlah dan kepelbagaian data; (ii) Tahap, kekerapan dan tempoh pemprosesan; (iii) Bilangan subjek data yang terlibat; (iv) Negara atau bidang kuasa di luar Malaysia yang terlibat dalam pemprosesan.
8.	Apakah **konteks Pemprosesan Dirancang**?	*Sila terangkan*	Ilustrasi dan contoh: Gambaran yang lebih luas, termasuk keadaan dalaman dan luaran yang mungkin mempengaruhi jangkaan dan impak. Pertimbangkan perkara berikut, jika berkenaan: (i) Sumber data peribadi;

Bil.	Soalan	Respons	Nota Panduan
			(ii) Sifat hubungan (organisasi) dengan subjek data; (iii) Tahap kawalan oleh subjek data terhadap data peribadi; (iv) Jangkaan subjek data terhadap pemprosesan tersebut; (v) Pengalaman terdahulu dengan jenis pemprosesan tersebut; (vi) Isu kepentingan awam semasa atau sensitiviti yang relevan dengan pemprosesan tersebut.
9.	Apakah **maksud** di sebalik **Pemprosesan Dirancang**?	*Sila terangkan* ("**Maksud**")	Ilustrasi: Sebab-sebab asas bagi pemprosesan tersebut dan hasil yang disasarkan untuk organisasi.
E – Menilai pematuhan, keperluan dan kekadaran			
10.	Apakah asas undang-undang yang terpakai di bawah Seksyen 6 Akta 709 untuk **pemprosesan data peribadi** dalam Pemprosesan Dirancang?	☐ Persetujuan subjek data ☐ Asas undang-undang lain di bawah subseksyen 6(2) Akta 709: *Sila nyatakan asas undang-undang yang terpakai* ☐ Pengecualian di bawah Seksyen 45 Akta 709: *Sila nyatakan pengecualian yang berkenaan*	Sila tandakan kotak pilihan yang berkenaan. Contoh asas undang-undang di bawah subseksyen 6(2) Akta 709: (i) Perlu bagi melaksanakan sesuatu kontrak yang subjek data itu ialah suatu pihak kepadanya; (ii) Perlu bagi mematuhi apa-apa obligasi undang-undang yang dikenakan ke atas pengawal data (selain daripada obligasi kontrak);

Bil.	Soalan	Respons	Nota Panduan
			(iii) Perlu bagi melindungi kepentingan vital (iaitu hal berkenaan kehidupan, kematian atau keselamatan) subjek data; (iv) Perlu bagi mentadbirkan keadilan.
11.	Jika Pemprosesan Dirancang melibatkan **pemprosesan data peribadi sensitif**, apakah asas undang-undang yang terpakai di bawah Seksyen 40 Akta 709?	☐ Tidak berkenaan ☐ Persetujuan secara nyata subjek data ☐ Asas undang-undang lain di bawah subseksyen 40(1) Akta 709: *Sila nyatakan asas undang-undang yang terpakai* ☐ Pengecualian di bawah Seksyen 45 Akta 709: *Sila nyatakan pengecualian yang berkenaan*	Sila tandakan kotak pilihan yang berkenaan. Contoh asas undang-undang di bawah subseksyen 40(1) Akta 709: (i) Perlu bagi maksud menjalankan atau melaksanakan apa-apa hak atau obligasi yang diberikan atau dikenakan oleh undang-undang terhadap pengawal data yang berkaitan dengan pengambilan kerja; (ii) Perlu bagi maksud mendapatkan nasihat undang-undang.
12.	Jika Pemprosesan yang Dirancang melibatkan **penzahiran data peribadi kepada pihak ketiga**, apakah asas undang-undang yang terpakai di bawah Seksyen 39 Akta 709?	☐ Tidak berkenaan ☐ Persetujuan subjek data ☐ Asas undang-undang lain di bawah Seksyen 39 Akta 709: *Sila nyatakan asas undang-undang yang terpakai* ☐ Pengecualian di bawah Seksyen 45 Akta 709: *Sila nyatakan pengecualian yang berkenaan*	Sila tandakan kotak pilihan yang berkenaan. Contoh asas undang-undang di bawah Seksyen 39 Akta 709: (i) Perlu bagi maksud mencegah atau mengesan suatu jenayah atau bagi maksud penyiasatan; (ii) Dikehendaki atau dibenarkan oleh atau di bawah mana-mana undang-undang atau oleh perintah suatu mahkamah.

Bil.	Soalan	Respons	Nota Panduan
13.	Jika Pemprosesan Dirancang melibatkan **pemindahan data peribadi ke suatu tempat di luar Malaysia**, apakah asas undang-undang yang terpakai di bawah Seksyen 129 Akta 709?	☐ Tidak berkenaan ☐ Negara penerima mempunyai undang-undang yang sebahagian besarnya serupa dengan Akta 709 ☐ Negara atau bidang kuasa penerima memastikan suatu tahap perlindungan yang mencukupi yang sekurang-kurangnya setara dengan Akta 709 ☐ Persetujuan subjek data terhadap pemindahan tersebut ☐ Asas undang-undang lain di bawah subseksyen 129(3) Akta 709: *Sila nyatakan asas undang-undang yang terpakai*	Sila tandakan kotak pilihan yang berkenaan. <u>Contoh asas undang-undang di bawah subseksyen 129(3) Akta 709</u>: (i) Perlu bagi pelaksanaan suatu kontrak antara subjek data dan pengawal data; (ii) Bagi maksud mana-mana prosiding undang-undang atau bagi maksud untuk mendapatkan nasihat undang-undang atau untuk mendapatkan nasihat undang-undang atau untuk mewujudkan, menjalankan melaksanakan atau mempertahankan hak di sisi undang-undang; (iii) Perlu bagi melindungi kepentingan vital (iaitu, hal berkenaan kehidupan, kematian atau keselamatan) subjek data.
14.	Adakah pengawal data berada dalam golongan Pengawal Data yang perlu berdaftar di bawah Akta 709?	☐ Ya ☐ Tidak	Sila tandakan kotak pilihan yang berkenaan. Jika “Tidak”, sila rujuk kepada Kod Tata Amalan Umum yang berkenaan. Jika “Ya”, teruskan ke Soalan 15.
15.	Adakah Pemprosesan Dirancang tertakluk kepada pematuhan mana-mana **Kod Tata Amalan** yang dikeluarkan oleh Pesuruhjaya?	☐ Ya ☐ Tidak *Sila nyatakan Kod Tata Amalan yang berkenaan* (“**Kod Tata Amalan**”)	Sila tandakan kotak yang berkenaan. Contoh Kod Tata Amalan yang dikeluarkan oleh Pesuruhjaya termasuk:

Bil.	Soalan	Respons	Nota Panduan
			(i) Kod Tata Amalan Perlindungan Data Peribadi untuk Sektor Pengangkutan Malaysia; (ii) Kod Tata Amalan Perlindungan Data Peribadi untuk Sektor Perbankan dan Institusi Kewangan; (iii) Kod Tata Amalan Perlindungan Data Peribadi untuk Industri Insurans dan Takaful di Malaysia; (iv) Kod Tata Amalan Perlindungan Data Peribadi untuk Sektor Komunikasi; (v) Kod Tata Amalan Perlindungan Data Peribadi untuk Sektor Utiliti (Elektrik); (vi) Kod Tata Amalan Perlindungan Data Peribadi untuk Sektor Utiliti (Air); (vii) Kod Tata Amalan Perlindungan Data Peribadi untuk Hospital Swasta dalam Industri Jagaan Kesihatan.
16.	Apakah **keperluan** di bawah Kod Tata Amalan yang terpakai yang mengawal selia Pemprosesan Dirancang dan bagaimakah pematuhan tersebut dipastikan?	Huraian: *Sila nyatakan*	Ilustrasi: Pengawal data hendaklah mengenal pasti keperluan khusus yang ditetapkan di bawah **Kod Tata Amalan** berkenaan Pemprosesan Dirancang. Ini termasuk apa-apa piawaian, langkah perlindungan dan kewajipan khusus sektor. Seterusnya, pengawal data hendaklah menilai dan mendokumentasikan bagaimana Pemprosesan Dirancang mematuhi keperluan tersebut.

Bil.	Soalan	Respons	Nota Panduan
17.	Adakah perlu menggunakan Pemprosesan Dirancang bagi mencapai maksud tersebut?	☐ Ya ☐ Tidak Huraian: *Sila nyatakan*	Sila tandakan kotak yang berkenaan. Ilustrasi dan contoh: Pertimbangkan sama ada terdapat cara lain yang munasabah untuk mencapai maksud **tanpa** menggunakan Pemprosesan Dirancang tersebut. Sebagai contoh: (i) Memanfaatkan kaedah sedia ada untuk mencapai maksud tersebut. (ii) Menentukan sama ada menyahnama data peribadi masih membolehkan maksud tersebut dicapai.
18.	Adakah wajar (berkadaran) untuk menggunakan Pemprosesan Dirancang bagi mencapai maksud tersebut?	☐ Ya ☐ Tidak Huraian: *Sila nyatakan*	Sila tandakan kotak pilihan yang berkenaan. Ilustrasi dan contoh: Pertimbangkan sama ada terdapat cara lain yang munasabah untuk mencapai maksud melalui Pemprosesan Dirancang tetapi melalui **tahap pemprosesan yang lebih terhad.** Sebagai contoh: (i) Mengurangkan jenis data peribadi yang dikumpul daripada subjek data; (ii) Mengurangkan tempoh pemprosesan atau penyimpanan; (iii) Mengurangkan takat atau menghentikan penzahiran data peribadi kepada pihak ketiga.

Bil.	Soalan	Respons	Nota Panduan
I – Mengenal pasti dan menganalisis risiko			

*Sila gunakan **matriks risiko** ini untuk mengenal pasti tahap risiko bagi setiap soalan dalam Soalan 19 hingga 29.*

Matriks Risiko		**Kebarangkalian**		
		Rendah (1)	**Sederhana (2)**	**Tinggi (3)**
Impak	**Tinggi (3)**	Sederhana (3)	Tinggi (6)	TInggi (9)
	Sederhana (2)	Rendah (2)	Sederhana (4)	Tinggi (6)
	Rendah (1)	Low (1)	Rendah (2)	Sederhana (3)

19.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **Prinsip Am** di bawah Seksyen 6 Akta 709?	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	<u>Contoh pertimbangan</u>: (i) Sama ada Pemprosesan yang Dirancang adalah bagi maksud yang sah yang berhubungan secara langsung dengan aktiviti pengawal data. (ii) Sama ada pemprosesan adalah perlu atau berhubungan secara langsung dengan maksud tersebut. (iii) Sama ada data peribadi adalah mencukupi tetapi tidak berlebihan berhubungan dengan maksud tersebut.

Bil.	Soalan	Respons	Nota Panduan
20.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **Prinsip Notis dan Pilihan** di bawah Seksyen 7 Akta 709?	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: (i) Sama ada notis bertulis sedia ada yang diberikan kepada subjek data adalah mencukupi untuk merangkumi Pemprosesan yang Dirancang tersebut. (ii) Bilakah notis bertulis tersebut diberikan atau bilakah ia akan diberikan kepada subjek data?
21.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **Prinsip Penzahiran** di bawah Seksyen 8 Akta 709?	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: Sama ada penzahiran data peribadi tersebut adalah bagi maksud selain daripada maksud bagi data peribadi itu dizahirkan pada masa pengumpulan atau maksud yang berkaitan secara langsung dengan maksud pada masa pengumpulan tersebut.
22.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **Prinsip Keselamatan** di bawah Seksyen 9 Akta 709?	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Huraian: Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: (i) Risiko kehilangan, salah guna, ubah suaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan data peribadi. (ii) Langkah-langkah praktikal yang diambil untuk melindungi data peribadi daripada risiko tersebut.
23.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **Prinsip Penyimpanan** di	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: (i) Sama ada data peribadi akan disimpan tidak lebih lama daripada yang diperlukan bagi memenuhi maksud tersebut.

Bil.	Soalan	Respons	Nota Panduan
	bawah Seksyen 10 Akta 709?		(ii) Sama ada data peribadi akan dipadamkan secara kekal sebaik sahaja data peribadi itu tidak lagi diperlukan untuk maksud tersebut.
24.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **Prinsip Integriti Data** di bawah Seksyen 11 Akta 709?	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: Sama ada langkah-langkah munasabah akan diambil untuk memastikan bahawa data peribadi adalah: (i) Tepat; (ii) Lengkap; (iii) Tidak mengelirukan; dan (iv) Terkini.
25.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **Prinsip Akses** di bawah Seksyen 12 Akta 709?	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: (i) Sama ada subjek data akan dapat mengakses data peribadinya di bawah Pemprosesan yang Dirancang bagi membolehkan pembetulan yang berkenaan. (ii) Sama ada Pemprosesan yang Dirancang akan menjejaskan keupayaan untuk mematuhi keperluan di bawah Seksyen 30 hingga 37 Akta 709.
26.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **hak-hak lain subjek data** di bawah Akta 709, khususnya	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: Sama ada subjek data akan dapat: (i) Menarik balik persetujuan.

Bil.	Soalan	Respons	Nota Panduan
	Seksyen-seksyen 38, 42, 43 dan 43A?		(ii) Menghalang pemprosesan yang mungkin menyebabkan kerosakan atau distres. (iii) Menghalang pemprosesan bagi maksud pemasaran langsung. (iv) Melaksanakan hak kemudahalihan data.
27.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar **keperluan lain** di bawah Akta 709, khususnya Seksyen-seksyen 12A, 12B, 25(2) dan 130?	☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	Contoh pertimbangan: (i) Sama ada Pemprosesan yang Dirancang memerlukan pelantikan DPO tambahan (contoh: disebabkan peningkatan dalam pemprosesan data peribadi atau pemantauan sistematik). (ii) Sama ada Pemprosesan yang Dirancang menjejaskan keupayaan untuk mematuhi keperluan mandatori pemberitahuan pelanggaran data. (iii) Sama ada Pemprosesan yang Dirancang mengakibatkan pelanggaran mana-mana peruntukan di bawah Kod Tata Amalan yang terpakai. (iv) Sama ada Pemprosesan yang Dirancang melibatkan pengumpulan data peribadi yang tidak sah.
28.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar keperluan khusus di bawah	☐ Rendah ☐ Sederhana ☐ Tinggi	Contoh pertimbangan: (i) Sama ada langkah perlindungan tambahan, langkah teknikal atau kawalan organisasi yang dikehendaki di

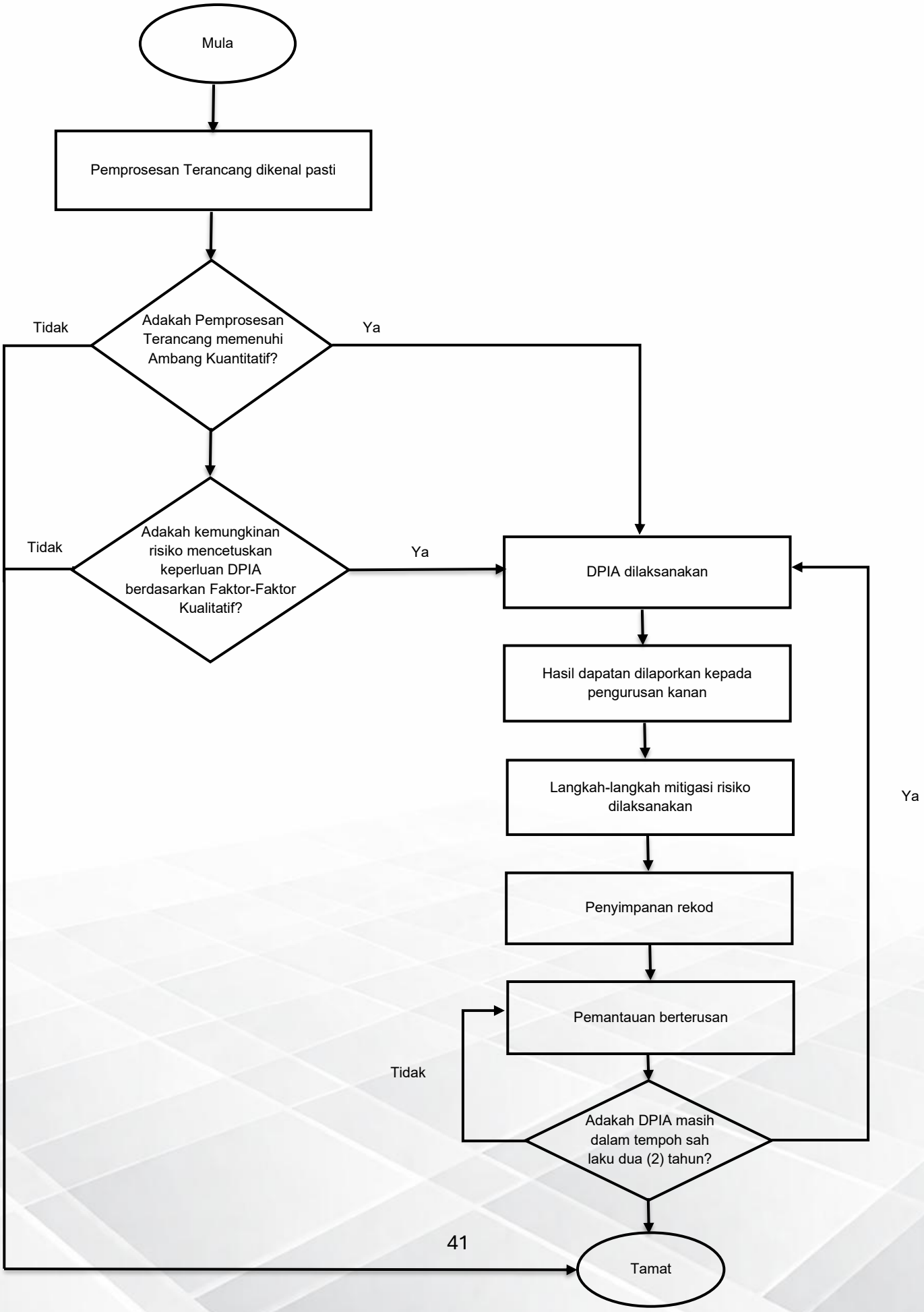
Bil.	Soalan	Respons	Nota Panduan
	Kod Tata Amalan yang berkenaan?	Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	bawah Kod Amalan yang berkenaan telah dilaksanakan (contoh: penyulitan dan langkah keselamatan data). (ii) Sama ada terdapat sebarang jurang antara Pemprosesan yang Dirancang dengan standard atau amalan terbaik yang ditetapkan di bawah Kod Amalan yang berkenaan. (iii) Sama ada proses yang sewajarnya telah diwujudkan untuk membolehkan subjek data tersebut melaksanakan hak selaras dengan keperluan khusus yang ditetapkan di bawah Kod Amalan yang berkenaan.
29.	Apakah **potensi impak dan kemudaratan** terhadap subjek data diakibatkan daripada Pemprosesan Dirancang serta tahap risiko tersebut? (Anda boleh menambahkan baris bagi setiap potensi impak dan kemudaratan yang dikenal pasti. Contoh: 29(a), 29(b) dan sebagainya.	Potensi impak/kemudaratan: *Sila huraikan.* ☐ Rendah ☐ Sederhana ☐ Tinggi Huraian: *Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.*	<u>Contoh potensi impak atau kemudaratan</u>: (i) Risiko keselamatan; (ii) Ketidakupayaan untuk melaksanakan hak subjek data; (iii) Kehilangan kawalan terhadap penggunaan data peribadi; (iv) Kecurian identiti atau penipuan; (v) Kerugian kewangan; (vi) Kecederaan fizikal; (vii) Kehilangan kerahsiaan; dan

Bil.	Soalan	Respons	Nota Panduan
			(viii) Undang-undang privasi dan perlindungan data yang tidak mencukupi di negara penerima pemindahan data peribadi.
C – Pertimbang langkah-langkah mitigasi risiko			
30.	Apakah langkah-langkah yang boleh (dan akan) diambil untuk mengurangkan risiko-risiko yang dinyatakan dalam soalan 19 hingga 29? (Anda boleh menambahkan baris bagi setiap langkah yang dikenal pasti. Contoh: 30(a), 30(b) dan sebagainya.)	Langkah: *Sila huraikan* Apakah risiko yang bakal dikurangkan oleh langkah ini: *Sila nyatakan nombor soalan yang berkaitan.* Tahap pengurangan risiko: ☐ Sebahagian ☐ Material ☐ Signifikan Individu yang bertanggungjawab melaksanakan langkah: *Sila nyatakan* Tarikh jangkaan siap pelaksanaan: *Sila nyatakan*	<u>Contoh langkah</u>: (i) Tidak mengumpul jenis data tertentu; (ii) Mengurangkan kekerapan pemprosesan atau memendekkan tempoh penyimpanan; (iii) Melaksanakan langkah-langkah keselamatan tambahan; (iv) Menyahnama *(anonymise)* atau menyamarkan *(pseudonymise)* data peribadi tertentu; (v) Menggunakan teknologi yang berbeza; (vi) Menerapkan perlindungan kontraktual tambahan dengan pihak ketiga yang terlibat dalam pemprosesan; dan (vii) Menjalankan Penilaian Impak Pemindahan (TIA) untuk menentukan sama ada pemindahan tersebut dibenarkan di bawah Akta 709 dan/atau negara

Bil.	Soalan	Respons	Nota Panduan
			penerima mempunyai undang-undang perlindungan data dan privasi yang mencukupi.
A – Taksir baki tahap risiko keseluruhan			
31.	Apakah tahap risiko sisa keseluruhan (dengan mengambil kira langkah yang akan dilaksanakan) bagi Pemprosesan Dirancang tersebut?	☐ Rendah ☐ Sederhana ☐ Tinggi	Penilaian terhadap: (i) tahap risiko yang ditetapkan bagi soalan 19 hingga 29; dan (ii) sejauh mana keberkesanan langkah yang dicadangkan tersebut dijangka secara realistik dapat mengurangkan risiko spesifik tersebut.
32.	Bilakah tarikh penyiapan DPIA?	*Sila nyatakan*	Ini merupakan tarikh permulaan bagi tempoh sah laku selama dua (2) tahun bagi DPIA tersebut.
<u>Pasca-DPIA</u>: Mengurus risiko dan kebertanggungjawaban (akauntabiliti)			
Pelaporan kepada pengurusan kanan			
33.	Sekiranya baki tahap risiko keseluruhan dinilai sebagai Tinggi, siapakah yang bertanggungjawab untuk melaporkan hasil dapatan DPIA yang dilaksanakan terhadap Pemprosesan Dirancang kepada pengurusan kanan untuk	☐ Tidak berkenaan ☐ Individu bertanggungjawab: *Sila nyatakan*	Orang yang bertanggungjawab boleh terdiri daripada DPO, Ketua Pelaksana DPIA atau kakitangan lain yang dilantik.

Bil.	Soalan	Respons	Nota Panduan
	pertimbangan dan input mereka?		
34.	Lanjutan kepada soalan 30, adakah terdapat sebarang langkah mitigasi risiko tambahan yang akan dilaksanakan?	☐ Ya ☐ Tidak Huraian: *Sila jelaskan langkah-langkah yang diambil dan bagi setiap langkah tersebut, kenal pasti individu yang bertanggungjawab bagi pelaksanaan serta tarikh jangkaan siap.*	Ini bertujuan untuk menyatakan sebarang langkah mitigasi risiko tambahan yang dikenal pasti selepas DPIA disiapkan, yang mungkin berdasarkan input daripada pengurusan kanan.
Penyimpanan Rekod			
35.	Siapakah yang bertanggungjawab untuk menyelenggara DPIA dan semua dokumen berkaitan dengan sewajarnya bagi tempoh sekurang-kurangnya dua (2) tahun dari tarikh penghentian operasi pemprosesan?	*Sila nyatakan*	Sila nyatakan nama kakitangan yang berkenaan. Sekiranya sesebuah pasukan bertanggungjawab, sila nyatakan nama ahli pasukan tersebut.

LAMPIRAN B : CARTA ALIR PELAKSANAAN DPIA



MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION

GUIDELINE

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Version 1.0

Date of Issuance: 30 April 2026

DEPARTMENT OF PERSONAL DATA PROTECTION

Address:

DEPARTMENT OF PERSONAL DATA PROTECTION
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 out the requirement for both the data controller and the data processor to appoint one or more Data Protection Officers ("**DPO**") to oversee their compliance with Act 709.

1.2 Pursuant to the Circular of Personal Data Protection Commissioner No. 1/2025 (Appointment of Data Protection Officer) and the Appointment of Data Protection Officer Guideline, one of the core responsibilities of a DPO is to support and advise on the carrying out of a Data Protection Impact Assessment ("**DPIA**").

1.3 This DPIA Guideline ("**Guideline**") provides practical guidance in relation to the carrying out of DPIA. Through this process, the organisations can systematically identify and manage risks associated with their personal data processing activities, ensuring that such activities comply with the requirements of Act 709.

1.4 Please note that examples provided in this Guideline are not intended to be exhaustive and are included solely for context illustration purposes.

1.5 This Guideline supplements and is to be read together with Act 709 and any other relevant legislative instrument(s) issued under Act 709, as may be amended from time to time. It This Guideline shall not be considered to override any other personal data protection-related laws and regulations in force.

2. Legal Provisions

2.1 This Guideline is issued by the Personal Data Protection Commissioner ("**Commissioner**") pursuant to the functions of the Commissioner under subsection 48(g) of Act 709. In accordance with subparagraph 5(1)(d) of the Circular of Commissioner of Data Protection No. 1/2025 (Appointment of Data Protection Officer), the Commissioner in this Guideline sets out the requirements in relation to the carrying out of DPIA.

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 Act 709 and any other relevant legislative instrument(s) issued under Act 709.

PART B: PRE-DPIA

4. What is a DPIA

4.1 A DPIA is an assessment of the impact of a planned processing operation on personal data protection. It involves identifying, assessing, and managing personal data protection risks based on the organisation's functions, requirements, and processes of an organisation.

4.2 In essence, DPIA is a process designed to analyse and mitigate personal data protection risks.

5. Why Carry Out a DPIA

5.1 DPIA serves as a useful mechanism to assist organisations in ascertaining the risks associated with a processing operation. It enables the organisation to evaluate whether such risks are acceptable in the circumstances, when weighed against the purpose and nature of the processing operation. By identifying risks at an early stage, organisations can determine and implement appropriate risk treatment measures, including preventive and mitigative measures to manage these risks and to ensure compliance with the Act 709. This proactive approach ensures effective risk management and full compliance with Act 709.

5.2 The implementation of a DPIA assists organisations in fulfilling the adequacy requirements prevalent in the international personal data protection landscape. For instance, the European Union, the United Kingdom, Indonesia, the Philippines, and South Korea have established the DPIA as a mandatory legal obligation under specific circumstances. Furthermore, DPIAs are expressly recommended as best practices in numerous other jurisdictions, including Singapore, Japan, Australia, and New Zealand.

5.3 Carrying out a DPIA will enhances an organisation's accountability and transparency. By demonstrating a steadfast commitment to safeguarding personal data, organisations can significantly bolster public confidence and foster long-term trust in their data processing activities.

6. Who Is Responsible for Carrying Out a DPIA

6.1 The obligation to carry out a DPIA falls on the data controller. This is because, by definition, the data processor does not process personal data for its own purposes and the data controller shall be responsible in deciding whether to proceed with a processing operation and ensure that all risks are addressed.

6.2 Nevertheless, the data processor who is involved in the processing operation is expected to provide all reasonable and necessary assistance to the data controller in carrying out the DPIA. The data controller shall reinforce this expectation through clear contractual clauses or other appropriate methods.

Duty to carry out DPIA

6.3 The ultimate responsibility for carrying out the DPIA and for any resulting decisions rests with the senior management of the data controller.

DPO vs DPIA Lead

6.4 One of the core responsibilities of a DPO is to support the carrying out of DPIA. In this regard, the DPO shall provide the following support:

(a) identifying whether a DPIA needs to be carried out;

(b) providing advice in relation to the carrying out of DPIA and the implementation of risk mitigation measures; and

(c) developing DPIA templates or checklists customised for the data controller.

6.5 The DPO may not necessarily be the individual leading the carrying out of a DPIA. A DPIA Lead may either be the DPO, the project manager, or other personnel deemed appropriate by the data controller ("**DPIA Lead**").

6.6 The DPIA Lead is the key personnel in charge of planning and executing the DPIA. This includes consulting and gathering input from relevant stakeholders on matters such as details of the processing operation, identified risks or challenges, and appropriate risk treatment solutions and mitigation measures to address those risks.

Stakeholder Engagement

6.7 To ensure a DPIA is comprehensive and effective, it shall involve all relevant stakeholders from various functions of the organisation connected with the processing operation. These include, but are not limited to:

(a) project manager;
(b) IT department;
(c) legal department;
(d) any other subject matter experts;
(e) data processor; and
(f) relevant third parties as defined under the Act 709.

6.8 All relevant stakeholders are expected to assist the DPO and the DPIA Lead and provide appropriate input in completing the DPIA.

7. When to Carry Out DPIA

7.1 A data controller shall carry out a DPIA if the data controller foresees that a processing operation is likely to result in a high risk to the protection of personal data for the data subject.

7.2 In this regard, the data controller is required to follow a two-tier approach to determine the level of risk and assess whether a DPIA is required:

(a) First, the data controller shall determine if the **quantitative threshold** (as explained in paragraph 7.5) is met. If the quantitative threshold is met, a DPIA shall be carried out.

(b) Second, if the quantitative threshold is not met, the DPO shall exercise best judgment in considering the **qualitative factors** (as explained in paragraph 7.6) to determine whether a DPIA is required.

7.3 This Guideline does not derogate from the requirements set out under any other legal or regulatory instruments regarding the circumstances in which a DPIA needs to be carried out. Where there is an overriding obligation imposed by those other instruments, that broader requirement shall apply.

7.4 In cases where it is not obvious whether a DPIA is required, it is prudent for the data controller to carry out a DPIA nonetheless as a best practice, as it remains a useful tool for building trust with the data subject, managing personal data protection risks, and facilitating compliance with the Act 709.

Quantitative Threshold

7.5 The following circumstances are deemed likely to result in a high risk to the protection of personal data for the data subject, thereby triggering the requirement to carry out a DPIA:

(a) processing of personal data expected to involve more than 20,000 data subjects; or

(b) processing of sensitive personal data, including financial information data, expected to involve more than 10,000 data subjects.

(collectively referred to as the "**Quantitative Thresholds**").

Qualitative Factors

7.6 If the processing does not meet any of the Quantitative Thresholds, the DPO is required to exercise best judgment in considering other qualitative factors that are likely to result in a high risk to the protection of personal data for the data subject, such that a DPIA is required to be carried out. It is emphasised that these qualitative factors are neither exhaustive nor exclusive and include but are not limited to, the following:

(a) potential legal or significant effects on the data subject (e.g., noticeable impact on the data subject's legal status or rights, financial status, health, reputation, access to services or other economic or social opportunities);

Examples:

(1) Example 1: Processing of sensitive personal data that may significantly affect a data subject's access to insurance

Situation: An insurance company collects and processes health-related information, such as medical history or data obtained from fitness tracking applications, to determine a data subject's insurance eligibility, set premium rates or coverage approval.

Why DPIA is required: The data controller shall conduct a DPIA because the processing involves sensitive personal data and potentially involves automated decision-making that has a significant impact on the data subject's access to insurance services.

(2) Example 2: Processing of personal financial data that may significantly affect a data subject's access to loan facilities

Situation: A financial institution uses an automated credit scoring system to assess loan or credit applications. The system automatically approves or rejects an application without human review, resulting in an immediate impact on the data subject's credit score, financial standing, and access to financial services.

Why DPIA is required: The processing involves automated decision-making based on personal and financial data, which may have a direct and significant effect on the data subject's economic rights and opportunities. Therefore, the data controller is required to carry out a DPIA.

(b) systematic monitoring of the data subject;

Examples:

(1) Example 1: Systematic monitoring of individuals in a commercial setting

Situation: A retail chain uses facial recognition technology in all its stores to identify repeat customers enrolled in its loyalty programme. When the data subject enters an outlet, the system automatically matches the data subject's facial image against stored records to provide personalised discounts based on shopping history.

Why DPIA is required: Although the purpose is to enhance customer experience and marketing efficiency, the processing involves systematic monitoring of the data subject in a commercial setting and the use of biometric data (facial features) for identification. Such processing may pose a high risk of misidentification, profiling or intrusion into the privacy of the data subject. Accordingly, prior to the implementation of the facial recognition technology, the data controller is required to carry out a DPIA.

(2) Example 2: Continuous tracking of the data subject's location and behaviour linked to commercial transactions

Situation: A food delivery company offers an in-app loyalty feature that tracks the data subject's geolocation data when the app is opened or when orders are placed. The system logs the delivery address, frequently patronised food vendors, time spent on the application and browsing behaviour. The system cross-references this information with past purchase records to identify behavioural patterns such as spending habits, meal timing and preferred food vendors. The company uses these insights to deliver targeted advertisements, and location-based promotions, thereby influencing the data subject's purchasing decisions and marketing outcomes.

Why DPIA is required: The processing involves continuous tracking of the data subject's location and behaviour linked to commercial transactions. Such systematic monitoring and profiling activities are likely to result in a high risk to the protection of personal data. Therefore, the data controller is required to carry out a DPIA.

(c) use of innovative technologies, namely technologies that involve a new or significantly improved product (goods or services), a new process, a new marketing method, a new organisational method in business practices, or a new workplace organisation or external relations;

Examples:

(1) Example 1: Enhancing Business Processes via Innovative Technology

Situation: A financial institution operates a mobile banking application that enables customers to perform commercial transactions such as fund transfers, bill payments and online purchases using biometric fingerprint authentication. The data controller subsequently decides to enhance this process by incorporating Artificial Intelligence-driven biometric authentication features, such as facial recognition to provide an additional layer of security.

Why DPIA is required: The processing involves technology that is new to the organisation. The transition to facial recognition increases the volume and complexity of sensitive personal data being processed. This change may pose a significant risk to the privacy of the data subject due to the increased use of sensitive personal data. Therefore, the data controller is required to carry out a DPIA.

(2) Example 2: Innovative Technology in Workplace Practices

Situation: An organisation currently uses manual methods to monitor employee performance. The data controller has decided to adopt an Artificial Intelligence (AI) system to automate performance monitoring. The AI system generates performance scores and behavioural summaries, which are subsequently used as the primary basis for decisions regarding promotion, reward or disciplinary decisions.

Why DPIA is required: The processing involves the implementation of technology that is new to the organisation's operational environment. The transition to automated monitoring may significantly affect the data subject's employment rights, professional reputation and privacy. Therefore, the data controller is required to carry out a DPIA.

(d) denial or restriction of rights of the data subject;

Examples:

(1) Example 1: Denial or restriction of access to services

Situation: An e-hailing service provider requires the data subject to consent to continuous behavioural tracking, such as real-time location monitoring, trip patterns and in-app interactions, as a mandatory condition for accessing its services. A data subject who declines to consent may be denied access to the services entirely (for example, unable to book a ride) or may face specific restrictions (such as being ineligible for discounts or promotional offers).

Why DPIA is required: This practice involves the denial or restriction of the data subject's rights, particularly the freedom to withhold or withdraw consent without detriment. Accordingly, the data controller is required to carry out a DPIA.

(2) Example 2: Systemic restriction the right of access

Situation: An e-commerce company enables the data subject to make purchases via its mobile application. However, when the data subject requests access to his personal data, such as purchase history or account details, the application does not provide a direct mechanism for submitting such a request. Instead, the data subject is redirected to an external e-mail address or a telephone number to submit the request.

Why DPIA is required: This practice creates administrative hurdles that deter the data subject from exercising his right to access personal data. Since this involves a systemic restriction on the fundamental rights of the data subject, the data controller is required to carry out a DPIA.

(e) tracking of the data subject's location or behaviour;

Examples:

(1) Example 1: Continuous tracking through a retail app

Situation: A retail company uses a mobile application to continuously tracks the data subject's geolocation, store movement paths and dwell time at specific aisles. The personal data is used to analyse the data subject's behaviour, optimise store layout and deliver targeted advertisements or promotions based on real-time movement patterns.

Why DPIA is required: Since the processing involves regular and systematic tracking of the data subject's location and behaviour, the data controller is required to carry out a DPIA.

(2) Example 2: Online click-path analytics

Situation: An e-commerce platform tracks the data subject's online behaviour such as browsing history, clicks, time spent on pages and purchase activity, to predict buying intent, personalise prices and deliver targeted advertisements.

Why DPIA is required: The processing involves systematic and continuous monitoring of data subject's behaviour for commercial and profiling purposes. This may significantly affect data subject's rights and accordingly, the data controller is required to carry out a DPIA.

(f) targeting of children or vulnerable individuals; and

Example:

Processing of children's personal data for advertising purposes

Situation: An educational institution through its technology platform, collects children's personal data and intends to publish advertisements within the platform.

Why DPIA is required: The processing involves children's personal data and profiling activities, particularly for advertising purposes. This may give rise to risks regarding the protection of children's rights and the potential commercial targeting of minors. Therefore, the data controller is required to carry out a DPIA.

(g) automated decision-making and profiling that pose a high risk to the data subject.

(collectively referred to as the "**Qualitative Factors**").

7.7 DPOs shall exercise their best judgment in considering the Qualitative Factors, which may include factors that are not expressly set out above, to determine whether a processing operation is likely to result in a high risk to the protection of personal data for the data subject.

Illustration: Determining the Necessity of Carrying Out a DPIA

(i) An organisation intends to store its customers' personal data with an external cloud service provider. Such proposed storage constitutes a processing operation.

Quantitative Threshold

(ii) The data controller of the organisation, in consultation with the DPO, shall first consider whether such processing operation meets the Quantitative Threshold (i.e., whether it is deemed likely to result in a high risk to the protection of personal data for the data subject), by asking the following questions:

a) Is the processing operation expected to involve more than 20,000 data subjects?

b) Is the processing operation of sensitive personal data, including financial information, expected to involve more than 10,000 data subjects?

If **either** of the above is answered '**Yes**', the DPIA Lead is required to carry out DPIA on the processing operation.

(iii) If **both** of the above are answered '**No**', the DPO, upon consultation with the DPIA Lead, shall exercise best judgement in considering the **Qualitative Factors** to determine whether the processing operation is likely to result in a high risk to the protection of personal data for the data subject.

Qualitative Factors

(iv) The relevant Qualitative Factors may include, for example:

a) the types of personal data involved (e.g., whether the processing may lead to potential legal or significant effects on the data subject); and

b) the location of cloud service provider (e.g., if the provider is located outside of Malaysia, whether such place has data protection laws equivalent to the Act 709 to safeguard the personal data).

(v) If, in the DPO's best judgment, the processing operation is likely to result in a high risk to the protection of personal data for the data subject, the DPIA Lead is required to carry out a DPIA.

(vi) If the DPO is of the view that the processing operation is unlikely to result in a high risk to the protection of personal data for the data subject, the DPO may advise that carrying out a DPIA to be done as a best practice.

PART C: CARRYING OUT A DPIA

8. How to Carry Out a DPIA

8.1 A data controller is expected to adopt a five-step approach, which are Describe, Evaluate, Identify, Consider and Assess or better known as its abbreviation, DEICA ("**DEICA**"), to analyse a processing operation in relation to its purposes, the specific risks and the measures to be taken:

(a) **Step 1: Describe** – Describe the processing operations (including the extent of personal data involved and the data flow) and the purposes of the processing;

Explanation:

This step involves describing the processing in terms of the following aspects:

(i) **Nature:** What is planned with the personal data. (e.g., how the personal data will be collected, stored, used, accessed and disclosed with relevant parties);

(ii) **Scope:** What the processing covers**.** (e.g., the volume and variety of the personal data, the extent, frequency and duration of the processing, the number of data subjects involved, the geographical area covered and whether there is cross border transfer);

(iii) **Context:** The wider picture that may affect expectations and impact. (e.g., the nature of the relationship with the data subject and any current issues of public concern); and

(iv) **Purposes:** The reason why the organisation wants to process the personal data, which may include the intended outcome for the data subject and the expected benefits for the organisation.

(b) **Step 2: Evaluate** – Evaluate the compliance, necessity, and proportionality of the processing operation in relation to its purposes;

Explanation:

This may involve considering:

(i) whether the organisation's plans actually help to achieve the intended purposes; and

(ii) whether there is any other reasonable way to achieve the same result without the proposed processing or with a lesser extent of processing (e.g., whether a cross border transfer is really necessary in the processing operation to achieve the intended purposes).

(c) **Step 3: Identify** – Identify and analyse the specific risks to the protection of personal data of the data subject;

Explanation:

This may involve considering the risk of breaching any personal data protection principles or other requirements under the Act 709, as well as the potential impact on the data subject and any harm that the processing may cause, for example:

(i) security risks (including sources of risk and the potential impact for each type of breach);
(ii) inability to exercise data subject's rights;
(iii) loss of control over the use of personal data;
(iv) identity theft or fraud;
(v) financial loss;
(vi) physical harm;
(vii) loss of confidentiality; and

(viii) inadequate privacy and data protection laws in the country to which the personal data is transferred.

The analysis of the specific risks identified shall consider both the **Likelihood** and **Impact** of the possible harm. A **3 x 3 Risk Matrix** (as shown below) is used to determine the risk level for each specific risk. The risk score is derived by multiplying the Likelihood score by the Impact score.

1. **Risk Matrix (3 x 3)**

   The table below is a sample 3 x 3 Risk Matrix for the calculation of risk levels. Each possible harm's risk is calculated by multiplying the Likelihood with the Impact of the possible harm.

Risk Matrix		**Likelihood**		
		Low (1)	**Medium (2)**	**High (3)**
Impact	**High (3)**	Medium (3)	High (6)	High (9)
	Medium (2)	Low (2)	Medium (4)	High (6)
	Low (1)	Low (1)	Low (2)	Medium (3)

2. **Definition of Criteria**

   a) **Likelihood**

   Likelihood assesses the probability or chance of a risk event (e.g., data breach, accidental disclosure, unauthorised access, or loss of personal data) occurring within a given timeframe or operational context.

Likelihood	**Criteria**
Low (1)	The event is unlikely or has a remote chance of occurring. Existing controls or systems are in place and are adequate to protect the data subject.

Medium (2)	The event is possible or is known to occur in the specific industry. Controls or systems are in place but may have limitations or weaknesses.
High (3)	The event is highly likely to occur or has occurred previously. Controls or systems have limitations or weaknesses and have significant vulnerabilities.

b) Impact

Impact refers to the seriousness of the potential harm to the data subject if the risk materialises. It focuses on whether the processing is likely to result in a high risk to the protection of personal data for the data subject.

Impact	Criteria
Low (1)	Unlikely to result in a material risk. The data involved is non-sensitive, and any breach would cause minimal inconvenience with no significant impact on the data subject's rights or interests.
Medium (2)	Likely to result in a risk. The processing may cause material but not irreversible harm, such as social embarrassment, minor financial loss, emotional distress, or limited loss of control.
High (3)	Likely to result in a high risk to the protection of personal data for the data subject. The harm may be significant or irreversible, including substantial financial loss, identity theft, discrimination, or reputational damage.

3. Risk Response and Risk Treatment

Risk Score	Level	Action Required
1-2	**Low**	**Monitor** – Risk is manageable. Continue monitoring through existing controls and standard operating procedures.
3-4	**Medium**	**Mitigate** – Strengthen mitigation measures. Implement additional technical and/or organisational controls to reduce the likelihood or impact.
6-9	**High**	**Mandatory Action** – Likely to result in a high risk to the data subject. A DPIA is required. Robust risk treatment measures shall be implemented.

Illustration: Risk Assessment for Identity Theft

The following example demonstrates how a specific risk is identified and analysed.

As an illustration, if a processing operation poses a specific risk of identity theft, the data controller shall consider:

(i) **The likelihood** (e.g., whether identity theft has previously occurred within the organisation, among its competitors in the same industry, or in similar processing operations);

(ii) **The impact** (e.g., taking into account the extent of the harm that may be caused, based on the types of personal data involved such as bank account numbers and the profile of the data subject);

(iii) **Assigning a risk level** (e.g., if the specific risk of identity theft is assessed as "Medium"(2) in likelihood and "High"(3) in impact severity, such risk would be considered "High Risk"(6).

In such circumstances, more robust mitigation measures shall be implemented in Step 4 (Consider), which may subsequently affect the overall residual risk level in Step 5 (Assess)).

(d) **Step 4: Consider** – Consider measures to be taken to address the specific risks identified to safeguard the protection of personal data; and

Explanation:

This may involve any of the following:

(i) not to collect certain types of data;

(ii) reduce the frequency of processing or shorten retention periods;

(iii) implement additional security measures;

(iv) anonymise or pseudonymise certain personal data;

(v) use a different technology;

(vi) incorporate additional contractual safeguards with the third party involved in the processing; and

(vii) conduct a Transfer Impact Assessment (TIA) to determine whether the transfer is permitted under Act 709 and/or the receiving country has adequate data protection and privacy laws.

(e) **Step 5: Assess** – Assess the overall residual risk level (e.g., high, medium, low) of the processing operation.

Explanation:

This may involve considering the risk level assigned for each specific risk identified and the proposed measures to address those specific risks, to determine the overall residual risk level.

8.2 To illustrate how the DEICA procedure may be applied, a DPIA Template is provided under **Annex A** as a reference. The suggested DPIA Template is intended for guidance, and usage of its contents is discretionary. The data controller may adapt this Template to suit its specific

needs or circumstances, develop its own template (adapted from this Template), or develop any accompanying checklist, so long as it is aligned with this Guideline.

PART D: POST-DPIA

9. Report to Senior Management

9.1 Upon completion of the DPIA, where the overall residual risk level is assessed as “High”, the findings shall be reported to the senior management of the organisation. Unless otherwise determined by the organisation, all risks, regardless of their level, shall also be reported to senior management to ensure that it remains fully informed of all identified risks.

9.2 The senior management shall consider the DPIA findings and provide input in connection with the processing operation. This may include:

(a) accepting the overall residual risk level arising from the processing operation;

(b) deciding on any additional mitigation measures to manage the risks; and

(c) allocating appropriate resources for implementing the risk mitigation measures.

10. Implementation of Risk Mitigation Measures

10.1 Once a decision has been made to proceed with the processing operation, the identified risk mitigation measures shall be implemented accordingly to address and manage the specific risks identified in the DPIA.

10.2 The DPIA Lead is the key personnel responsible for overseeing the implementation of the risk mitigation measures. The DPO shall provide support and advice on such implementation in line with the organisation's data protection policies, industry best practices, and Act 709. The ultimate responsibility for implementing the risk mitigation measures, however, rests with the senior management of the data controller.

11. Publication, Validity and Monitoring

11.1 To promote transparency and accountability, the data controller may consider publishing its DPIA to foster trust in its personal data processing activities. To protect commercially sensitive information or manage other data security risks (including those involving personal data), the published DPIA may be redacted. Alternatively, a summary of the DPIA may be published.

11.2 A completed DPIA is **valid for a period of two (2) years** from its date of completion. Upon **expiry of that period**, **a refreshed DPIA** shall be carried out.

11.3 In any event, a DPIA is not a one-off activity but requires continuous monitoring and periodic review. Notwithstanding the validity period, and throughout the duration of the processing operation, the DPIA Lead shall monitor developments that may affect the processing operation, the risks identified and the risk mitigation measures adopted (e.g., changes to the purposes of processing or newly identified vulnerabilities in the technology used). The DPIA Lead shall address such developments accordingly to ensure the ongoing protection of the data subject.

12. Record-Keeping

12.1 In any event, the DPIA shall be carried and all relevant documentation shall be properly maintained for at least two (2) years from the cessation of the processing operation. For example, if the processing operation lasts for five (5) years, the DPIA and its relevant records shall be retained for two (2) years from the cessation of processing operation. Accordingly, the record-keeping period will be at least seven (7) years.

12.2 Such records shall be made available for inspection upon request by the Commissioner.

ANNEX A: DPIA TEMPLATE

No.	Questions	Responses	Guidance Notes
<u>Pre-DPIA</u>: Determine whether a DPIA is required			
Planned processing			
1.	What is the planned processing operation of personal data about?	*Please provide a brief explanation* ("**Planned Processing**")	<u>Response example</u>: *Engaging a human resource service provider, Z, to analyse customers' survey responses and store their personal data in Singapore.*
Determinants			
2.	Does the Planned Processing involve personal data expected to exceed 20,000 data subjects?	☐ Yes ☐ No Elaboration: *Please provide*	Please tick the applicable checkbox for each question. <u>Response examples for the elaboration</u>: i. The Planned Processing involves the processing of personal data exceeding 20,000 data subjects; or ii. The Planned Processing involves the processing of sensitive personal data, including financial information, exceeding 10,000 data subjects.
3.	Does the Planned Processing involve sensitive personal data including financial data, expected to exceed 10,000 data subjects?	☐ Yes ☐ No Elaboration: *Please provide*	

No.	Questions	Responses	Guidance Notes
4.	Does the Planned Processing involve **any Qualitative Factors** that will likely result in a high risk to the protection of personal data for the data subject, such that, in the DPO's judgment **a DPIA shall be carried out to further assess the risks?**	☐ Potential legal or significant effects on the data subject ☐ Systematic monitoring of the data subject ☐ Use of innovative technology ☐ Denial or restriction of the rights of data subject ☐ Tracking of the data subject's location or behaviour ☐ Targeting of children or other vulnerable individuals ☐ Automated decision-making and profiling that pose a high risk to the data subject ☐ Any other factors necessitating the carrying out of a DPIA: *Please elaborate* ☐ None of the above applies.	Please tick all applicable checkbox(es). Examples: (i) Potential legal or significant effects on the data subject (e.g., noticeable impact on the data subject's legal status or rights, financial status, health, reputation, access to services or other economic or social opportunities). (ii) Systematic monitoring of the data subject (*e.g., systematic monitoring of individuals in a commercial setting).* (iii) Use of innovative technology (*e.g., significantly improved business process through innovative technology).* (iv) Denial or restriction of the right of the data subject (*e.g., systemic restriction to the right of access).* (v) Tracking of data subject's location or behaviour *(e.g., online click-path analytics).* (vi) Targeting of children or other vulnerable individuals (*e.g., processing their personal data to offer services to them).* (vii) Automated decision-making and profiling that pose a high risk to the data subject.

No.	Questions	Responses	Guidance Notes
			(viii) Any other factors necessitating the carrying out of a DPIA (*e.g., risk of physical harm to the data subject in the event of data breach).*
Outcome			
5.	Does the Planned Processing require a DPIA?	☐ Yes ☐ No	Please tick "No", if: (i) questions 2 and 3 are responded with "No"; **AND** (ii) question 4 is responded with "None of the above applies". Otherwise, please tick "Yes" and proceed to answer the questions below.
DPIA: Carry out the five steps under DEICA			
D – Describe the Planned Processing			
6.	What is the **nature** of the Planned Processing?	*Please describe*	Illustration and examples: The description shall address what is planned to be done with the personal data: (iii) How the data will be collected; (iv) How the data will be stored; (v) How the data will be used; (vi) Who will have access to the data; (vii) To whom the data will be disclosed;

No.	Questions	Responses	Guidance Notes
			(viii) Whether any data processor will be engaged; (ix) The applicable retention period(s); (x) Security measures to be implemented.
7.	What is the **scope** of the Planned Processing?	*Please describe*	Illustration and examples: The description shall address what the processing covers, for example: (i) Volume and variety of the data; (ii) Extent, frequency, and duration of the processing; (iii) Number of data subjects involved; (iv) Countries or jurisdictions outside Malaysia involved in the processing.
8.	What is the **context** of the Planned Processing?	*Please describe*	Illustration and examples: The wider picture, including internal and external circumstances that may affect expectations and impact. Consider the following, where applicable: (i) Source of the personal data; (ii) Nature of the relationship with the data subject; (iii) The extent of control the data subject retains over the personal data;

No.	Questions	Responses	Guidance Notes
			(iv) Likely expectations the data subject has of the processing; (v) Previous experience with this type of processing; (vi) Current issues of public concern or sensitivity relevant to the processing.
9.	What are the **purposes** behind the Planned Processing?	*Please describe* ("**Purposes**")	Illustration: The underlying reason(s) for the processing and the intended outcome(s) for the organisation.
E – Evaluate compliance, necessity and proportionality			
10.	What is the applicable legal basis under Section 6 of the Act 709 for **processing personal data** under the Planned Processing?	☐ Consent of the data subject ☐ Another legal basis under subsection 6(2) of the Act 709: *Please state the applicable legal basis* ☐ Exempted under Section 45 of the Act 709: *Please state which exemption*	Please tick the applicable checkbox. Examples of legal basis under subsection 6(2) of the Act 709: (i) Necessary for the performance of a contract to which the data subject is a party; (ii) Necessary for compliance with any legal obligation to which the data controller is the subject (other than an obligation imposed by a contract); (iii) Necessary in order to protect the vital interests (i.e., matters relating to life, death or security) of the data subject; (iv) Necessary for the administration of justice.

No.	Questions	Responses	Guidance Notes
11.	If the Planned Processing involves **processing sensitive personal data**, what is the applicable legal basis under Section 40 of the Act 709?	☐ Not applicable ☐ Explicit consent of the data subject ☐ Another legal basis under subsection 40(1) of the Act 709: *Please state the applicable legal basis* ☐ Exempted under Section 45 of the Act 709: *Please state the applicable exemption*	Please tick the applicable checkbox. Examples of legal basis under subsection 40(1) of the Act 709: (i) Necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment; (ii) Necessary for the purpose of obtaining legal advice.
12.	If the Planned Processing involves **disclosing personal data to any third party**, what is the applicable legal basis under Section 39 of the Act 709?	☐ Not applicable ☐ Consent of the data subject ☐ Another legal basis under Section 39 of the Act 709: *Please state the applicable legal basis* ☐ Exempted under Section 45 of the Act 709: *Please state the applicable exemption*	Please tick the applicable checkbox. Examples of legal basis under Section 39 of the Act 709: (i) Necessary for the purpose of preventing or detecting a crime or for the purpose of investigations; (ii) Required or authorised by or under any law or by the order of a court.
13.	If the Planned Processing involves **transferring personal data to a place outside Malaysia**, what is the applicable legal basis under Section 129 of the Act 709?	☐ Not applicable ☐ The recipient country has a law substantially similar to the Act 709	Please tick the applicable checkbox. Examples of legal basis under subsection 129(3) of the Act 709: (i) Necessary for the performance of a contract between the data subject and the data controller;

No.	Questions	Responses	Guidance Notes
		☐ The recipient country or jurisdiction ensures an adequate level of protection equivalent to the Act 709. ☐ Consent of the data subject to the transfer ☐ Another legal basis under subsection 129(3) of the Act 709: *Please state the applicable legal basis*	(ii) For the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; (iii) Necessary in order to protect the vital interests (i.e., matters relating to life, death or security) of the data subject.
14.	Does the data controller belong to a class of data controllers required to be registered under Act 709?	☐ Yes ☐ No	Please tick the applicable checkbox. If "No", please refer to the General Code of Practice, where applicable. If "Yes", proceed to Question 15.
15.	Is the Planned Processing subject to compliance with any applicable **Code of Practice** issued by the Commissioner?	☐ Yes ☐ No *Please specify the applicable Code of Practice* ("**Code of Practice**")	Please tick the applicable checkbox. Examples of Codes of Practice issued by the Commissioner include: (i) Personal Data Protection Code of Practice for the Malaysia Aviation Sector; (ii) Personal Data Protection Code of Practice for the Banking and Financial Institutions Sector; (iii) Personal Data Protection Code of Practices for the Insurance and Takaful Industry in Malaysia;

No.	Questions	Responses	Guidance Notes
			(iv) Personal Data Protection Code of Practice for the Communications Sector; (v) Personal Data Protection Code of Practice for the Utilities Sector (Electricity); (vi) Personal Data Protection Code of Practice for the Utilities Sector (Water); (vii) Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry.
16.	What are the **requirements** under the applicable Code of Practice which governs the Planned Processing, and how is compliance ensured?	Elaboration: *Please provide*	Illustration: The data controller shall identify the specific requirements set out in the Code of Practice with regards to the Planned Processing. This includes any standards, safeguards and sector-specific obligations. Next, the data controller shall assess and document how the Planned Processing complies with said requirements.
17.	Is it **necessary** to adopt the Planned Processing in order to achieve the Purposes?	☐ Yes ☐ No Elaboration: *Please provide*	Please tick the applicable checkbox. Illustration and examples: Consider whether there is any other reasonable way to achieve the Purposes **without** adopting the Planned Processing. For example: (i) Leveraging on existing means to achieve the Purposes;

<table>
<tr><th>No.</th><th>Questions</th><th>Responses</th><th>Guidance Notes</th></tr>
<tr><td></td><td></td><td></td><td>(ii) Determining whether anonymising personal data would still enable the Purposes to be achieved.</td></tr>
<tr><td>18.</td><td>Is it proportionate to adopt the Planned Processing to achieve the Purposes?</td><td>☐ Yes ☐ No

Elaboration: Please provide</td><td>Please tick the applicable checkbox.

<u>Illustration and examples</u>: Consider whether there is any other reasonable way to achieve the Purposes through the Planned Processing, but via a lesser extent of processing. For example:

(i) Collecting fewer types of personal data from the data subject;

(ii) Reducing the duration of processing or retention;

(iii) Reducing the extent of or removing disclosure of personal data to a third party.</td></tr>
<tr><td colspan="4">I – Identify and analyse risks</td></tr>
<tr><td colspan="4">Please use this risk matrix to determine the risk level for each of Questions 19 to 29.

<table>
<tr><th colspan="2" rowspan="2">Risk Matrix</th><th colspan="3">Likelihood</th></tr>
<tr><th>Low (1)</th><th>Medium (2)</th><th>High (3)</th></tr>
<tr><td>I
m</td><td>High (3)</td><td>Medium (3)</td><td>High (6)</td><td>High (9)</td></tr>
</table>
</td></tr>
</table>

No.	Questions	Responses	Guidance Notes

	p a c t	**Medium (2)**	Low (2)	Medium (4)	High (6)
		Low (1)	Low (1)	Low (2)	Medium (3)

19.	What is the extent of risk of the Planned Processing violating the **General Principle** under Section 6 of the Act 709?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	<u>Examples of consideration</u>: (i) Whether the Planned Processing is for a lawful purpose directly related to an activity of the data controller. (ii) Whether processing is necessary for or directly related to that purpose. (iii) Whether the personal data is adequate but not excessive in relation to that purpose.
20.	What is the extent of risk of the Planned Processing violating the **Notice and Choice Principle** under Section 7 of the Act 709?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	<u>Examples of consideration</u>: (i) Whether the existing written notice provided to the data subject is sufficient to cover the Planned Processing. (ii) When was the written notice provided or when will the written notice be provided to the data subject?
21.	What is the extent of risk of the Planned Processing violating the **Disclosure**	☐ Low ☐ Medium ☐ High	<u>Example of consideration</u>: Whether the disclosure of personal data is for any other purpose than the purpose for which the personal data was

No.	Questions	Responses	Guidance Notes
	Principle under Section 8 of the Act 709?	Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	to be disclosed at the time of collection or a purpose directly related to the purpose at the time of collection.
22.	What is the extent of risk of the Planned Processing violating the **Security Principle** under Section 9 of the Act 709?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	Examples of consideration: (i) The risks of loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction of personal data. (ii) The practical steps taken to protect personal data from those risks.
23.	What is the extent of risk of the Planned Processing violating the **Retention Principle** under Section 10 of the Act 709?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	Examples of consideration: (i) Whether the personal data will be kept no longer than is necessary for the fulfilment of the Purposes. (ii) Whether the personal data will be permanently deleted once it is no longer required for the Purposes.
24.	What is the extent of risk of the Planned Processing violating the **Data Integrity Principle** under Section 11 of the Act 709?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	Examples of consideration: *Whether reasonable steps will be taken to ensure that the personal data is:* (i) Accurate; (ii) Complete; (iii) Not misleading; and (iv) Kept up-to-date.

No.	Questions	Responses	Guidance Notes
25.	What is the extent of risk of the Planned Processing violating the **Access Principle** under Section 12 of the Act 709?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	Examples of consideration: (i) Whether the data subject will be able to access their personal data under the Planned Processing to enable any applicable correction. (ii) Whether the Planned Processing will affect the ability to comply with the requirements under Sections 30 to 37 of the Act 709.
26.	What is the extent of risk of the Planned Processing violating **other data subject rights** under the Act 709, particularly Sections 38, 42, 43 and 43A?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	Examples of consideration: Whether the data subject will be able to: (i) Withdraw consent. (ii) Prevent processing likely to cause damage or distress. (iii) Prevent processing for direct marketing. (iv) Exercise the right to personal data portability.
27.	What is the extent of risk of the Planned Processing violating **other requirements** under the Act 709, particularly Sections 12A, 12B, 25(2) and 130?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	Examples of consideration: (i) Whether the Planned Processing necessitates the need to appoint additional DPOs (e.g., due to an increase in the processing of personal data or systematic monitoring).

No.	Questions	Responses	Guidance Notes
			(ii) Whether the Planned Processing affects the ability to comply with the mandatory data breach notification requirements. (iii) Whether the Planned Processing results in a breach of any provisions under the applicable Code of Practice. (iv) Whether the Planned Processing constitutes an unlawful collection of personal data.
28.	What is the extent of risk of the Planned Processing breaching the **specific requirements** of the applicable Code of Practice?	☐ Low ☐ Medium ☐ High Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	<u>Examples of consideration</u>: (i) Whether additional safeguards, technical measures, or organisational controls required under the applicable Code of Practice have been implemented (e.g., encryption, data security safeguards). (ii) Whether there are any gaps between the Planned Processing and the standards or best practices prescribed under the applicable Code of Practice. (iii) Whether appropriate processes are in place to enable the data subject to exercise rights in accordance with the specific requirements set out in the applicable Code of Practice.
29.	What are the **potential impacts and harms** on the data subject that the Planned Processing may cause and their extent of	Potential impact/harm: *Please explain.* ☐ Low ☐ Medium ☐ High	<u>Examples of potential impact or harm</u>: (i) Security risks; (ii) Inability to exercise data subject's rights;

No.	Questions	Responses	Guidance Notes
	risk? (You may add additional rows for each potential impact and harm identified, e.g. 29(a), 29(b) and etc.)	Elaboration: *Please explain as appropriate and specify the likelihood and impact severity*	(iii) Loss of control over the use of personal data; (iv) Identity theft or fraud; (v) Financial loss; (vi) Physical harm; (vii) Loss of confidentiality; and (viii) Inadequate data and privacy protection laws in the country to which the data is transferred.
C – Consider measures to mitigate risks			
30.	What are the measures that can (and will) be adopted to mitigate the risks set out under questions 19 to 29? (You may add additional rows for each measure identified, e.g. 30(a), 30(b) and etc.)	Measure: *Please explain* Which risk(s) does the measure mitigate: *Please state the question number(s)* Degree of mitigating the risk(s): ☐ Some ☐ Material ☐ Significant Responsible person to implement the measures: *Please state* Expected completion date of the implementation: *Please state*	Examples of measures: (i) Not to collect certain types of data; (ii) Reduce the frequency of processing or shorten retention periods; (iii) Implement additional security measures; (iv) Anonymise or pseudonymise certain personal data (v) Use a different technology; (vi) Incorporate additional contractual safeguards with the third party involved in the processing; and (vii) Conduct a Transfer Impact Assessment to determine whether the transfer is permitted under Act 709 and/or

No.	Questions	Responses	Guidance Notes
			the receiving country has adequate data protection and privacy laws.
A – Assess overall residual risk level			
31.	What is the overall residual risk level (taking into account the measures to be implemented) of the Planned Processing?	☐ Low ☐ Medium ☐ High	Evaluation of: (i) the risk levels assigned under questions 19 to 29; and (ii) how effective the proposed measures are realistically expected to mitigate these specific risks.
32.	What is the date of completing the DPIA?	*Please state*	This will be the starting date of the two (2) year validity period of the DPIA.
Post-DPIA: Manage risks and accountability			
Report to senior management			
33.	If the overall residual risk level is assessed as High, who is responsible for reporting the findings of the DPIA carried out on the Planned Processing to the senior management for its consideration and input?	☐ Not applicable ☐ Responsible person: *Please state*	The responsible person can be the DPO, the DPIA Lead or another designated personnel.
34.	Further to question 30, are there any additional risk	☐ Yes ☐ No Elaboration: *Please describe the measures and for each measure, identify the*	This is to set out any additional risk mitigation measures that are identified after the completion of the DPIA, which

No.	Questions	Responses	Guidance Notes
	mitigation measures that will be implemented?	*responsible person for implementation and the expected completion date of the implementation.*	may or may not be based on input from the senior management.
Record keeping			
35.	Who is responsible for properly maintaining the DPIA and all relevant documents for at least two (2) years from the cessation of the processing operation?	*Please provide*	Please provide the name(s) of the personnel. If a team is responsible, please provide the names of the team members.

ANNEX B: FLOWCHART ON CARRYING OUT A DPIA