



KEMENTERIAN DIGITAL



GARIS PANDUAN PERLINDUNGAN DATA PERIBADI

PENILAIAN IMPAK PERLINDUNGAN DATA (DPIA)



Versi 1.0
Tarikh Terbitan: 30 April 2026

JABATAN PERLINDUNGAN DATA PERIBADI



Hak Cipta Terpelihara
(Jabatan Perlindungan Data Peribadi, 2026)

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

BIL.	PERKARA	MUKA SURAT
BAHAGIAN A: PENGENALAN		3
1.	Latar Belakang	3
2.	Peruntukan Undang-Undang	3
3.	Tafsiran	4
BAHAGIAN B: PRA-DPIA		4
4.	Apakah itu DPIA	4
5.	Mengapa Melaksanakan DPIA	4
6.	Siapa Yang Bertanggungjawab Melaksanakan DPIA	5
7.	Bilakah Perlu Melaksanakan DPIA	6
BAHAGIAN C: PELAKSANAAN DPIA		15
8.	Cara Melaksanakan DPIA	15
BAHAGIAN D: PASCA-DPIA		21
9.	Laporan kepada Pengurusan Kanan	21
10.	Pelaksanaan Langkah Mitigasi Risiko	22
11.	Penerbitan, Kesahan dan Pemantauan	22
12.	Penyimpanan Rekod	23
LAMPIRAN A: TEMPLAT DPIA		24
LAMPIRAN B: CARTA ALIR PELAKSANAAN DPIA		41

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 melengkap 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 Iwn 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 pemrosesan 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 eksklusif 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: Pemrosesan 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 pemrosesan tersebut melibatkan data peribadi sensitif dan pembuatan keputusan secara automatik yang memberi kesan signifikan kepada akses subjek data terhadap perlindungan insurans.

(2) Contoh 2: Pemrosesan 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: Pemrosesan 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 kesetiannya. 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 pemrosesan adalah untuk meningkatkan pengalaman pelanggan dan kecekapan pemasaran, pemrosesan ini melibatkan pemantauan sistematik terhadap subjek data dalam persekitaran komersial dan penggunaan data biometrik (ciri wajah) untuk pengecaman. Pemrosesan 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 berpacuan 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 menggunakan sistem Kecerdasan Buatan (AI) bagi mengautomatiskan 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) penyesaran 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 penyesaran 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.

Ilustrasi: 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 rendah (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)
I m p a k	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 pribadi 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.

Ilustrasi: Penilaian Risiko bagi Kecurian Identiti

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 Pemandangan (TIA) untuk menentukan sama ada pemandangan 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 penyediaan. 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 pemrosesan 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 pemrosesan. Sebagai contoh, jika operasi pemrosesan 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: Menentukan sama ada DPIA diperlukan</u>			
Pemprosesan Dirancang			
1.	Apakah maksud dan operasi pemprosesan data peribadi yang dirancang?	<i>Sila berikan penjelasan ringkas</i> ("Pemprosesan Dirancang")	<i>Contoh respons: Melantik penyedia perkhidmatan sumber manusia, Z, untuk menganalisis maklum balas tinjauan pelanggan dan menyimpan data peribadi mereka di Singapura.</i>
Penentu			
2.	Adakah Pemprosesan Dirancang tersebut melibatkan data peribadi yang dijangka melebihi 20,000 subjek data?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak Penjelasan: <i>Sila berikan</i>	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?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak Penjelasan: <i>Sila berikan</i>	

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

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

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?	<i>Sila terangkan</i>	<u>Ilustrasi dan contoh:</u> 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?	<i>Sila terangkan</i>	<u>Ilustrasi dan contoh:</u> Gambaran yang lebih luas, termasuk keadaan dalaman dan luaran yang mungkin mempengaruhi jangkauan 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 ?	<i>Sila terangkan</i> ("Maksud")	<u>Ilustrasi</u> : 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?	<input type="checkbox"/> Persetujuan subjek data <input type="checkbox"/> Asas undang-undang lain di bawah subseksyen 6(2) Akta 709: <i>Sila nyatakan asas undang-undang yang terpakai</i> <input type="checkbox"/> Pengecualian di bawah Seksyen 45 Akta 709: <i>Sila nyatakan pengecualian yang berkenaan</i>	Sila tandakan kotak pilihan yang berkenaan. <u>Contoh asas undang-undang di bawah subseksyen 6(2) Akta 709:</u> (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
			<p>(iii) Perlu bagi melindungi kepentingan vital (iaitu hal berkenaan kehidupan, kematian atau keselamatan) subjek data;</p> <p>(iv) Perlu bagi mentadbirkan keadilan.</p>
11.	<p>Jika Pemprosesan Dirancang melibatkan pemprosesan data peribadi sensitif, apakah asas undang-undang yang terpakai di bawah Seksyen 40 Akta 709?</p>	<p><input type="checkbox"/> Tidak berkenaan</p> <p><input type="checkbox"/> Persetujuan secara nyata subjek data</p> <p><input type="checkbox"/> Asas undang-undang lain di bawah subseksyen 40(1) Akta 709: <i>Sila nyatakan asas undang-undang yang terpakai</i></p> <p><input type="checkbox"/> Pengecualian di bawah Seksyen 45 Akta 709: <i>Sila nyatakan pengecualian yang berkenaan</i></p>	<p>Sila tandakan kotak pilihan yang berkenaan.</p> <p><u>Contoh asas undang-undang di bawah subseksyen 40(1) Akta 709:</u></p> <p>(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;</p> <p>(ii) Perlu bagi maksud mendapatkan nasihat undang-undang.</p>
12.	<p>Jika Pemprosesan yang Dirancang melibatkan penzahiran data peribadi kepada pihak ketiga, apakah asas undang-undang yang terpakai di bawah Seksyen 39 Akta 709?</p>	<p><input type="checkbox"/> Tidak berkenaan</p> <p><input type="checkbox"/> Persetujuan subjek data</p> <p><input type="checkbox"/> Asas undang-undang lain di bawah Seksyen 39 Akta 709: <i>Sila nyatakan asas undang-undang yang terpakai</i></p> <p><input type="checkbox"/> Pengecualian di bawah Seksyen 45 Akta 709: <i>Sila nyatakan pengecualian yang berkenaan</i></p>	<p>Sila tandakan kotak pilihan yang berkenaan.</p> <p><u>Contoh asas undang-undang di bawah Seksyen 39 Akta 709:</u></p> <p>(i) Perlu bagi maksud mencegah atau mengesan suatu jenayah atau bagi maksud penyiasatan;</p> <p>(ii) Dikehendaki atau dibenarkan oleh atau di bawah mana-mana undang-undang atau oleh perintah suatu mahkamah.</p>

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?	<input type="checkbox"/> Tidak berkenaan <input type="checkbox"/> Negara penerima mempunyai undang-undang yang sebahagian besarnya serupa dengan Akta 709 <input type="checkbox"/> Negara atau bidang kuasa penerima memastikan suatu tahap perlindungan yang mencukupi yang sekurang-kurangnya setara dengan Akta 709 <input type="checkbox"/> Persetujuan subjek data terhadap pemindahan tersebut <input type="checkbox"/> Asas undang-undang lain di bawah subseksyen 129(3) Akta 709: <i>Sila nyatakan asas undang-undang yang terpakai</i>	<p>Sila tandakan kotak pilihan yang berkenaan.</p> <p><u>Contoh asas undang-undang di bawah subseksyen 129(3) Akta 709:</u></p> <p>(i) Perlu bagi pelaksanaan suatu kontrak antara subjek data dan pengawal data;</p> <p>(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;</p> <p>(iii) Perlu bagi melindungi kepentingan vital (iaitu, hal berkenaan kehidupan, kematian atau keselamatan) subjek data.</p>
14.	Adakah pengawal data berada dalam golongan Pengawal Data yang perlu berdaftar di bawah Akta 709?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak	<p>Sila tandakan kotak pilihan yang berkenaan.</p> <p>Jika “Tidak”, sila rujuk kepada Kod Tata Amalan Umum yang berkenaan.</p> <p>Jika “Ya”, teruskan ke Soalan 15.</p>
15.	Adakah Pemprosesan Dirancang tertakluk kepada pematuhan mana-mana Kod Tata Amalan yang dikeluarkan oleh Pesuruhjaya?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak <i>Sila nyatakan Kod Tata Amalan yang berkenaan</i> (“Kod Tata Amalan”)	<p>Sila tandakan kotak yang berkenaan.</p> <p>Contoh Kod Tata Amalan yang dikeluarkan oleh Pesuruhjaya termasuk:</p>

Bil.	Soalan	Respons	Nota Panduan
			<ul style="list-style-type: none"> (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: <i>Sila nyatakan</i>	<p><u>Ilustrasi:</u></p> <p>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.</p>

Bil.	Soalan	Respons	Nota Panduan
17.	Adakah perlu menggunakan Pemprosesan Dirancang bagi mencapai maksud tersebut?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak Huraian: <i>Sila nyatakan</i>	Sila tandakan kotak yang berkenaan. <u>Ilustrasi dan contoh:</u> 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?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak Huraian: <i>Sila nyatakan</i>	Sila tandakan kotak pilihan yang berkenaan. <u>Ilustrasi dan contoh:</u> 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 <i>matriks risiko</i> ini untuk mengenal pasti tahap risiko bagi setiap soalan dalam Soalan 19 hingga 29.																								
		<table border="1"> <thead> <tr> <th colspan="2" rowspan="2">Matriks Risiko</th> <th colspan="3">Kebarangkalian</th> </tr> <tr> <th>Rendah (1)</th> <th>Sederhana (2)</th> <th>Tinggi (3)</th> </tr> </thead> <tbody> <tr> <th rowspan="3">I m p a k</th> <th>Tinggi (3)</th> <td>Sederhana (3)</td> <td>Tinggi (6)</td> <td>Tinggi (9)</td> </tr> <tr> <th>Sederhana (2)</th> <td>Rendah (2)</td> <td>Sederhana (4)</td> <td>Tinggi (6)</td> </tr> <tr> <th>Rendah (1)</th> <td>Low (1)</td> <td>Rendah (2)</td> <td>Sederhana (3)</td> </tr> </tbody> </table>		Matriks Risiko		Kebarangkalian			Rendah (1)	Sederhana (2)	Tinggi (3)	I m p a k	Tinggi (3)	Sederhana (3)	Tinggi (6)	Tinggi (9)	Sederhana (2)	Rendah (2)	Sederhana (4)	Tinggi (6)	Rendah (1)	Low (1)	Rendah (2)	Sederhana (3)
Matriks Risiko		Kebarangkalian																						
		Rendah (1)	Sederhana (2)	Tinggi (3)																				
I m p a k	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?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<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?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> (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?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> 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?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Huraian: Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> (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 bawah Seksyen 10 Akta 709?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> (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?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> 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?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> (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	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> 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 distress. (iii) Menghalang pemprosesan bagi maksud pemasaran langsung. (iv) Melaksanakan hak kemudahan data.
27.	Sejauh manakah tahap risiko Pemprosesan Dirancang melanggar keperluan lain di bawah Akta 709, khususnya Seksyen-seksyen 12A, 12B, 25(2) dan 130?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<u>Contoh pertimbangan:</u> (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	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi	<u>Contoh pertimbangan:</u> (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: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i>	<p>bawah Kod Amalan yang berkenaan telah dilaksanakan (contoh: penyulitan dan langkah keselamatan data).</p> <p>(ii) Sama ada terdapat sebarang jurang antara Pemprosesan yang Dirancang dengan standard atau amalan terbaik yang ditetapkan di bawah Kod Amalan yang berkenaan.</p> <p>(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.</p>
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.	<p>Potensi impak/kemudaratan: <i>Sila huraikan.</i></p> <p><input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> Tinggi</p> <p>Huraian: <i>Sila jelaskan mengikut kesesuaian dan nyatakan kebarangkalian serta keseriusan impak.</i></p>	<p><u>Contoh potensi impak atau kemudaratan:</u></p> <p>(i) Risiko keselamatan;</p> <p>(ii) Ketidakupayaan untuk melaksanakan hak subjek data;</p> <p>(iii) Kehilangan kawalan terhadap penggunaan data peribadi;</p> <p>(iv) Kecurian identiti atau penipuan;</p> <p>(v) Kerugian kewangan;</p> <p>(vi) Kecederaan fizikal;</p> <p>(vii) Kehilangan kerahsiaan; dan</p>

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.)	<p>Langkah: <i>Sila huraikan</i></p> <p>Apakah risiko yang bakal dikurangkan oleh langkah ini: <i>Sila nyatakan nombor soalan yang berkaitan.</i></p> <p>Tahap pengurangan risiko: <input type="checkbox"/> Sebahagian <input type="checkbox"/> Material <input type="checkbox"/> Signifikan</p> <p>Individu yang bertanggungjawab melaksanakan langkah: <i>Sila nyatakan</i></p> <p>Tarikh jangkaan siap pelaksanaan: <i>Sila nyatakan</i></p>	<p><u>Contoh langkah:</u></p> <p>(i) Tidak mengumpul jenis data tertentu;</p> <p>(ii) Mengurangkan kekerapan pemrosesan atau memendekkan tempoh penyimpanan;</p> <p>(iii) Melaksanakan langkah-langkah keselamatan tambahan;</p> <p>(iv) Menyahnama (<i>anonymise</i>) atau menyamarkan (<i>pseudonymise</i>) data peribadi tertentu;</p> <p>(v) Menggunakan teknologi yang berbeza;</p> <p>(vi) Menerapkan perlindungan kontraktual tambahan dengan pihak ketiga yang terlibat dalam pemrosesan; dan</p> <p>(vii) Menjalankan Penilaian Impak Pemindahan (TIA) untuk menentukan sama ada pemindahan tersebut dibenarkan di bawah Akta 709 dan/atau negara</p>

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?	<input type="checkbox"/> Rendah <input type="checkbox"/> Sederhana <input type="checkbox"/> 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?	<i>Sila nyatakan</i>	Ini merupakan tarikh permulaan bagi tempoh sah laku selama dua (2) tahun bagi DPIA tersebut.
<u>Pasca-DPIA: Mengurus risiko dan kebertanggungjawaban (akauntabiliti)</u>			
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	<input type="checkbox"/> Tidak berkenaan <input type="checkbox"/> Individu bertanggungjawab: <i>Sila nyatakan</i>	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?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak Huraian: <i>Sila jelaskan langkah-langkah yang diambil dan bagi setiap langkah tersebut, kenal pasti individu yang bertanggungjawab bagi pelaksanaan serta tarikh jangkaan siap.</i>	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?	<i>Sila nyatakan</i>	Sila nyatakan nama kakitangan yang berkenaan. Sekiranya sesebuah pasukan bertanggungjawab, sila nyatakan nama ahli pasukan tersebut.

LAMPIRAN B : CARTA ALIR PELAKSANAAN DPIA

