KERTAS KONSULTASI AWAM NO. 1/2025

GARIS PANDUAN PENILAIAN IMPAK PERLINDUNGAN DATA

Tarikh Mula: 20 Mac 2025

Tarikh Akhir: 19 Mei 2025

BAHAGIAN 1: PENGENALAN DAN LATAR BELAKANG

1.1 Akta Perlindungan Data Peribadi (Pindaan) 2024 memperkenalkan Seksyen 12A baharu dalam Akta Perlindungan Data Peribadi 2010 ("**Akta 709**") yang menetapkan keperluan mandatori bagi pengawal data dan pemproses data untuk melantik seorang Pegawai Perlindungan Data ("**DPO**").

1.2 Teks penuh Seksyen 12A Akta 709 adalah seperti berikut:

> ***Pelantikan Pegawai Perlindungan Data***
>
> ***12A.*** *(1) Seseorang pengawal data hendaklah melantik seorang atau lebih pegawai perlindungan data yang hendaklah bertanggungan kepada pengawal data bagi pematuhan Akta ini.*
>
> *(2) Jika pemprosesan data peribadi dijalankan oleh seorang pemproses data bagi pihak pengawal data, pemproses data hendaklah melantik seorang atau lebih pegawai perlindungan data yang hendaklah bertanggungan kepada pemproses data bagi pematuhan Akta ini.*
>
> *(3) Pengawal data itu hendaklah memberitahu Pesuruhjaya tentang pelantikan pegawai perlindungan data mengikut cara dan dalam bentuk yang ditentukan oleh Pesuruhjaya.*
>
> *(4) Pelantikan pegawai perlindungan data di bawah subseksyen (1) dan (2) tidak melepaskan pengawal data atau pemproses data daripada semua kewajipan dan fungsi di bawah Akta ini.*

1.3 Salah satu tanggungjawab DPO ialah memberi sokongan dan nasihat mengenai pelaksanaan penilaian impak perlindungan data ("**DPIA"**).

1.4 Bagi membimbing DPO dalam melaksanakan DPIA, Garis Panduan Penilaian Impak Perlindungan Data ("**Garis Panduan DPIA**") sedang dibangunkan oleh Pesuruhjaya Perlindungan Data Peribadi ("**Pesuruhjaya**") untuk menetapkan keperluan minimum serta langkah praktikal dalam mengurus dan melindungi data peribadi yang dikawal oleh sesebuah organisasi.

1.5 DPIA boleh membantu organisasi mengenal pasti secara sistematik potensi risiko yang berkaitan dengan aktiviti pemprosesan data mereka. Dengan mengenal pasti risiko lebih awal, organisasi boleh melaksanakan langkah pencegahan untuk menguruskan risiko tersebut. DPIA juga dapat meningkatkan keyakinan awam terhadap organisasi sambil menggalakkan akauntabiliti dan ketelusan.

1.6 Pelaksanaan DPIA selari dengan landskap rangka peraturan perlindungan data di peringkat global. Sebagai contoh, Kesatuan Eropah ("**EU**"), United Kingdom ("**UK**"), Indonesia dan Filipina telah menjadikan DPIA sebagai kewajipan undang-undang dalam keadaan tertentu. DPIA juga secara jelas disyorkan oleh badan pengawal selia di banyak negara lain termasuk Jepun, Korea Selatan, Singapura, New Zealand dan Australia.

1.7 Berdasarkan perkara di atas, Kertas Konsultasi Awam mengenai Garis Panduan DPIA ("**KKA**") ini bertujuan untuk mengumpulkan pandangan dan maklum balas orang awam mengenai aspek yang akan atau seharusnya dimasukkan dalam Garis Panduan DPIA yang dicadangkan.

BAHAGIAN 2: KEPERLUAN YANG DICADANGKAN UNTUK DPIA DI BAWAH AKTA 709

2.1 Sebagai gambaran keseluruhan, Bahagian 2 dalam KKA ini dikategorikan seperti berikut:

(a) Definisi;
(b) Siapakah yang perlu melaksanakan DPIA;
(c) Bilakah DPIA perlu dilaksanakan;
(d) Bagaimanakah cara untuk melaksanakan DPIA;
(e) Pemberitahuan kepada Pesuruhjaya; dan
(f) Tindakan selepas DPIA dilaksanakan.

[A] Definisi

2.2 **Latar belakang:** DPIA tidak disebut secara jelas dalam Akta 709. Oleh itu, adalah bermanfaat untuk menyediakan definisi bagi DPIA. Namun, definisi ini hanya bertujuan sebagai ilustrasi dan bukan untuk menetapkan skop DPIA secara menyeluruh.

2.3 **Cadangan:** Takrifan DPIA yang dicadangkan di bawah adalah berdasarkan definisi DPIA di UK dan Singapura. Definisi ini dicadangkan bagi memastikan keselarian dengan standard antarabangsa yang sentiasa berkembang berkaitan DPIA dan hal yang berkaitan.

Definisi

Penilaian Impak Perlindungan Data (DPIA) ialah penilaian terhadap impak operasi pemprosesan yang dirancang terhadap perlindungan data peribadi, yang mungkin melibatkan pengenalpastian, penilaian dan pengendalian risiko perlindungan data peribadi berdasarkan fungsi, keperluan dan proses organisasi

Soalan 1

Apakah pandangan anda mengenai skop definisi DPIA yang dicadangkan? Adakah definisi ini terlalu luas, atau adakah ia perlu dihadkan lagi?

[B] Siapakah yang perlu melaksanakan DPIA

2.4 **Latar belakang:** Di EU, UK, Singapura dan Indonesia, undang-undang mewajibkan pengawal data untuk melaksanakan DPIA dalam keadaan tertentu manakala di Filipina, pendekatan

yang lebih luas digunakan dengan mewajibkan pengawal data dan pemproses data untuk melaksanakan DPIA.

2.5 Bagi Malaysia, walaupun Seksyen 12A Akta 709 yang baharu mewajibkan pemproses data untuk melantik DPO, mereka tidak semestinya diwajibkan untuk menjalankan DPIA. Ini kerana, secara definisi, pemproses data tidak memproses data peribadi untuk tujuan mereka sendiri, sebaliknya keputusan untuk meneruskan operasi pemprosesan data adalah tanggungjawab pengawal data. Selain itu, mewajibkan pemproses data untuk menjalankan DPIA mungkin kurang praktikal memandangkan skop tanggungjawab undang-undang mereka di bawah Akta 709 adalah terhad.

2.6 **Cadangan:** Dicadangkan **bahawa hanya pengawal data** yang tertakluk kepada keperluan DPIA di bawah Akta 709.

Soalan 2

Apakah pandangan anda mengenai keperluan bahawa hanya pengawal data (dan bukan pemproses data) menjalankan DPIA?

[C] Bilakah DPIA perlu dilaksanakan?

2.7 **Latar belakang:** DPIA biasanya dilaksanakan oleh pengawal data untuk menentukan sama ada sesuatu pemprosesan [1] **berkemungkinan menimbulkan risiko tinggi terhadap perlindungan data peribadi bagi subjek data.**

2.8 Daripada bidang kuasa yang dikenal pasti, terdapat 2 pendekatan utama bagi pengawal data untuk menentukan kemungkinan risiko dalam menilai keperluan DPIA:

(a) faktor kualitatif (EU dan UK); dan

(b) ambang kuantitatif (Korea Selatan).

2.9 **Cadangan:** Memandangkan konsep DPIA masih baharu di Malaysia, dicadangkan bahawa pengawal data diwajibkan menjalankan DPIA dengan mengguna pakai pendekatan 2 peringkat yang mengambil kira ambang kuantitatif dan faktor kualitatif seperti berikut:

(i) Pertama, pengawal data perlu menentukan sama ada ambang kuantitatif telah dipenuhi. Jika ambang ini dipenuhi, maka DPIA wajib dilaksanakan.

[1] "Pemprosesan" ditakrifkan secara luas di bawah Akta 709 sebagai "mengumpul, merekod, memegang atau menyimpan data peribadi atau menjalankan apa-apa pengendalian atau set pengendalian terhadap data peribadi, termasuk (a) penyusunan, penyesuaian atau pengubahan data peribadi;b) mendapatkan kembali, merujuk kepada atau menggunakan data peribadi; (c) penzahiran data peribadi melalui penghantaran, pemindahan, penyebaran atau selainnya menjadikannya tersedia; atau (d) penjajaran, penggabungan, pembetulan, pemadaman atau pemusnahan data peribadi.

(ii) Kedua, jika ambang kuantitatif tidak dipenuhi, DPO masih perlu menggunakan pertimbangan terbaik mereka untuk menilai faktor kualitatif dan menentukan sama ada DPIA perlu dilaksanakan.

2.10 Dalam menilai ambang kuantitatif, **setiap** keadaan berikut **dianggap berkemungkinan menimbulkan risiko tinggi** terhadap perlindungan data peribadi bagi subjek data:

(a) pemprosesan **data peribadi[2] sensitif** yang dijangka melibatkan lebih daripada **10,000 subjek data**;

(b) pemprosesan **data peribadi untuk tujuan pembuatan keputusan secara automatik** (akan ditakrifkan oleh Pesuruhjaya) yang dijangka melibatkan lebih daripada **10,000 subjek data**; atau

(c) pemprosesan **data peribadi** yang dijangka melibatkan lebih daripada **20,000 subjek data**.

(secara kolektif dirujuk sebagai "**Ambang Kuantitatif**").

2.11 Perhatikan bahawa walaupun sesuatu pemprosesan tidak memenuhi Ambang Kuantitatif, **DPO** masih **bertanggungjawab untuk menggunakan pertimbangan terbaik *(best judgment)*** mereka dalam menilai faktor kualitatif lain bagi menentukan sama ada DPIA perlu dilaksanakan, termasuk:

(a) implikasi undang-undang atau kesan ketara yang berkemungkinan terhadap subjek data (contohnya, impak yang jelas terhadap status/hak undang-undang individu, kedudukan kewangan, kesihatan, reputasi, akses kepada perkhidmatan atau peluang ekonomi dan sosial lain);

(b) pemantauan sistematik di kawasan awam yang boleh diakses (contohnya, penggunaan CCTV dengan keupayaan pemprofilan);

(c) penggunaan teknologi inovatif (contohnya, gabungan cap jari dan pengecaman wajah untuk meningkatkan kawalan akses);

(d) penafian atau sekatan terhadap hak subjek data (contohnya, penggunaan pembuatan keputusan automatik untuk meluluskan atau menolak permohonan pinjaman/insurans);

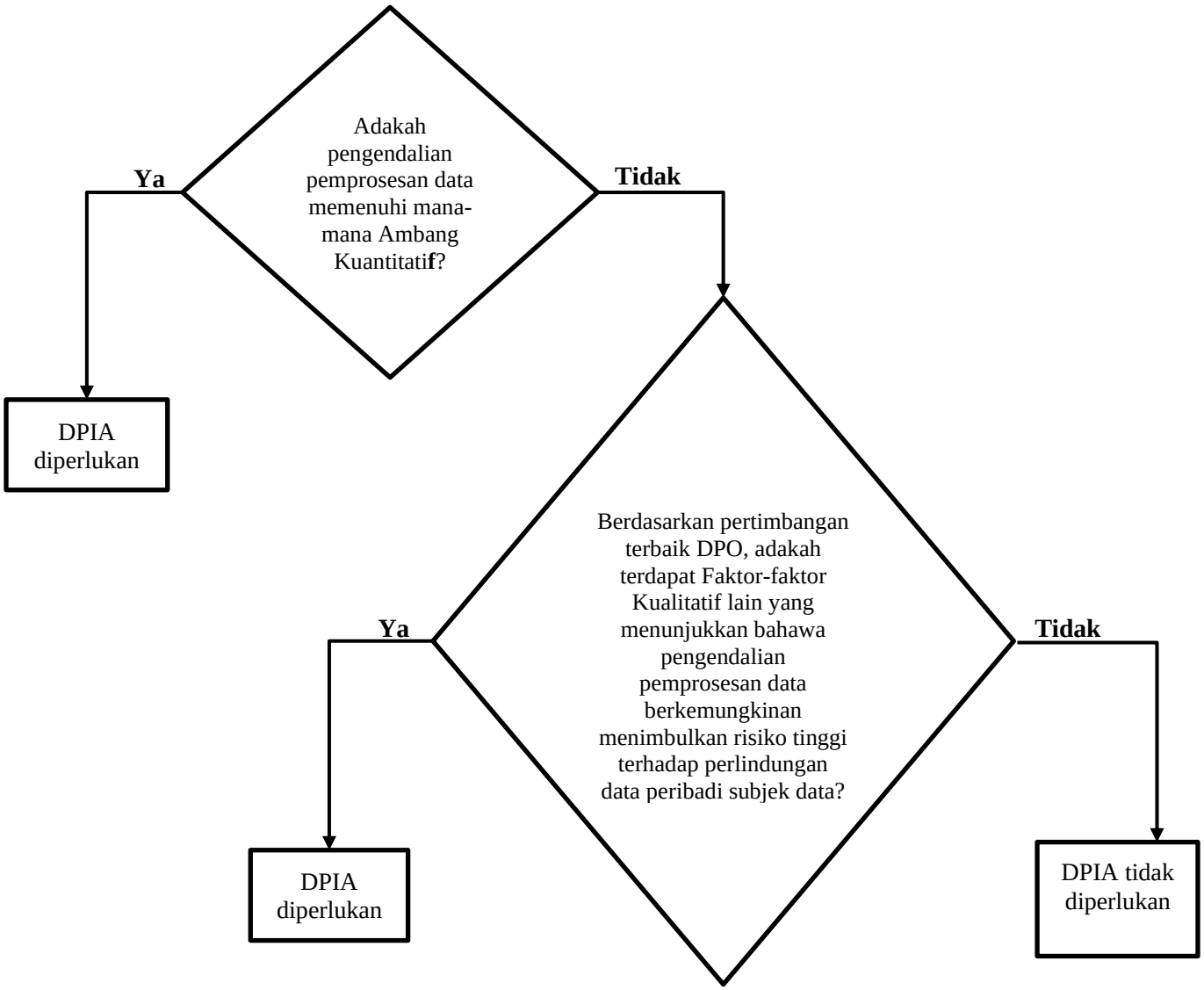
(e) penjejakan lokasi atau tingkah laku subjek data (contohnya, teknologi penjejakan mata untuk menjana data bagi menyediakan pemasaran langsung yang lebih diperibadikan); atau

[2] Di bawah Akta 709, "data peribadi sensitif" merangkumi "apa-apa data peribadi yang mengandungi maklumat tentang kesihatan atau keadaan fizikal atau mental seorang subjek data, pendapat politiknya, kepercayaan agamanya atau kepercayaan lain yang bersifat seumpanya, pelakuan atau pengataan pelakuan apa-apa kesalahan olehnya". Definisi ini juga merangkumi data biometrik, yang ditakrifkan sebagai "sebarang data peribadi yang terhasil daripada pemprosesan teknikal berkaitan dengan ciri fizikal, fisiologi, atau tingkah laku seseorang individu".

(f) penyasaran terhadap kanak-kanak atau individu rentan lain (contohnya, pemprosesan data peribadi mereka untuk menawarkan perkhidmatan khusus kepada mereka).

(secara kolektif dirujuk sebagai "**Faktor-faktor Kualitatif**").

2.12 Rasional di sebalik cadangan di atas dapat digambarkan seperti berikut:



Contoh

(i) Sebuah organisasi bercadang untuk menyimpan data peribadi pelanggan mereka dengan penyedia perkhidmatan awan luaran *(external cloud service provider)*. Penyimpanan data ini merupakan satu bentuk pengendalian pemprosesan.

Ambang Kuantitatif

(ii) DPO organisasi tersebut harus terlebih dahulu menilai sama ada pengendalian pemprosesan ini memenuhi Ambang Kuantitatif (iaitu, berkemungkinan

menimbulkan risiko tinggi terhadap perlindungan data peribadi subjek data) dengan menjawab soalan berikut:

- Adakah pengendalian pemprosesan ini melibatkan data peribadi sensitif dengan lebih daripada 10,000 subjek data yang dijangka terjejas?

- Adakah pengendalian pemprosesan ini bertujuan untuk pembuatan keputusan automatik dan dijangka melibatkan lebih daripada 10,000 subjek data?

- Adakah pengendalian pemprosesan ini dijangka melibatkan lebih daripada 20,000 subjek data?

(iii) Jika jawapan kepada **mana-mana** tiga soalan di atas adalah "**ya**", maka DPO wajib menjalankan DPIA ke atas pengendalian pemprosesan tersebut.

(iv) Jika jawapan kepada semua tiga soalan di atas adalah "**tidak**", DPO perlu menggunakan pertimbangan terbaik untuk menilai Faktor-faktor Kualitatif bagi menentukan sama ada pengendalian pemprosesan ini tetap berisiko tinggi terhadap perlindungan data peribadi subjek data.

Faktor-faktor Kualitatif

(v) Contoh Faktor-faktor Kualitatif yang relevan mungkin termasuk jenis data peribadi yang terlibat (contohnya, sama ada kemungkinan implikasi undang-undang atau kesan ketara terhadap subjek data); dan lokasi penyedia perkhidmatan awan (contohnya, jika terletak di luar Malaysia, adakah negara tersebut mempunyai undang-undang perlindungan data yang setara dengan Akta 709 untuk melindungi data peribadi).

(vi) Jika berdasarkan pertimbangan terbaik DPO pengendalian pemprosesan yang dicadangkan berkemungkinan menimbulkan risiko tinggi terhadap perlindungan data peribadi subjek data maka DPO wajib menjalankan DPIA.

(vii) Sebaliknya, jika DPO berpendapat bahawa pengendalian pemprosesan tersebut tidak berisiko tinggi terhadap perlindungan data peribadi subjek data, maka DPIA tidak perlu dilaksanakan.

Soalan 3

Dalam memberikan respons kepada soalan-soalan di bawah, sila berikan justifikasi yang jelas untuk menyokong pandangan anda:

(a) Berdasarkan cadangan dalam Perenggan 2.9, adakah anda bersetuju dengan penggunaan pendekatan dua peringkat: Ambang Kuantitatif dan Faktor-faktor Kualitatif di Malaysia? Sila nyatakan sebab dan cadangan anda.

(b) Apakah pandangan anda mengenai penggunaan Ambang Kuantitatif sebagai panduan dalam penilaian keperluan DPIA berbanding hanya bergantung sepenuhnya pada Faktor-faktor Kualitatif?

(c) Adakah anda menganggap angka yang dicadangkan dalam Perenggan 2.10 untuk Ambang Kuantitatif sebagai angka yang sesuai dan dianggap berkemungkinan membawa risiko tinggi terhadap perlindungan data peribadi subjek data? Jika jawapan anda tidak, sila nyatakan sebab.

Sebagai rujukan, Korea Selatan mewajibkan agensi kerajaan menjalankan DPIA sekiranya pemprosesan melibatkan 50,000 subjek data yang terdiri daripada maklumat sensitif atau maklumat peribadi yang boleh dikenal pasti.

(d) Apakah pandangan anda mengenai penggunaan pertimbangan terbaik DPO dalam menentukan keperluan untuk menjalankan DPIA berdasarkan Faktor-faktor Kualitatif?

(e) Selain daripada menilai DPIA berdasarkan Faktor-faktor Kualitatif dalam Perenggan 2.11, apakah faktor lain yang boleh dipertimbangkan / dicadangkan?

[D] Bagaimanakah cara untuk melaksanakan DPIA

2.13 **Latar belakang**: Pendekatan dalam melaksanakan DPIA adalah lebih kurang sama di negara lain. Ia merangkumi proses mengenal pasti, menilai dan menangani risiko perlindungan data peribadi dengan dokumentasi yang sewajarnya.

2.14 Sebagai gambaran, EU mewajibkan DPIA untuk mengandungi sekurang-kurangnya perkara berikut:

(a) huraian sistematik mengenai pengendalian pemprosesan dan tujuan pemprosesan, termasuk, jika berkenaan, kepentingan sah yang dijalankan oleh pengawal data;

(b) penilaian keperluan dan kesesuaian pengendalian pemprosesan berhubungan dengan tujuan pemprosesan;

(c) penilaian risiko terhadap hak dan kebebasan subjek data; dan

(d) langkah-langkah yang dirancang untuk menangani risiko, termasuk perlindungan, langkah keselamatan dan mekanisme bagi memastikan perlindungan data peribadi serta pematuhan terhadap peraturan EU dengan mengambil kira hak dan kepentingan sah subjek data serta pihak lain yang berkenaan.

2.15 **Cadangan**: Setelah meneliti pelbagai pendekatan yang berbeza tetapi secara umumnya serupa dalam bidang kuasa yang dikenal pasti, dicadangkan agar Malaysia mengguna pakai

pendekatan 5 langkah, yang disingkatkan sebagai "**DEICA**", bagi menganalisis pengendalian pemprosesan data berkaitan tujuan, risiko khusus dan langkah-langkah yang perlu diambil.

(a) "**Describe**": Huraikan pengendalian pemprosesan (termasuk, sebagai contoh, skop data peribadi yang terlibat dan aliran data) serta tujuan pemprosesan;

Penerangan:

Ia mungkin melibatkan penjelasan mengenai pemprosesan:

- sifat (antara lain, apa yang dirancang untuk dilaksanakan dengan data peribadi cth., bagaimana data dikumpul, disimpan dan digunakan, siapa yang mempunyai akses serta kepada siapa data dikongsi dan sebagainya);
- skop (antara lain, apa liputan pemprosesan cth., jumlah dan jenis data peribadi, tahap, kekerapan dan tempoh pemprosesan, bilangan subjek data yang terlibat, kawasan geografi yang diliputi, sama ada terdapat pemindahan rentas sempadan);
- konteks (antara lain, gambaran lebih luas yang mungkin mempengaruhi jangkaan dan impak cth., sifat hubungan dengan subjek data serta apa-apa isu semasa yang menjadi perhatian umum dan sebagainya); dan
- tujuan (antara lain, sebab sesebuah organisasi ingin memproses data peribadi, yang mungkin termasuk hasil yang diharapkan untuk subjek data serta manfaat yang dijangka bagi organisasi dan pihak lain).

(b) "**Evaluate**": Menilai keperluan dan kesesuaian pengendalian pemprosesan berhubung dengan tujuan pemprosesan;

Penerangan:

Ini mungkin melibatkan pertimbangan:

- Sama ada perancangan organisasi benar-benar membantu mencapai tujuan yang dimaksudkan.
- Sama ada terdapat cara lain yang munasabah untuk mencapai hasil yang sama tanpa pemprosesan yang dicadangkan atau dengan tahap pemprosesan yang lebih rendah (contohnya, adakah pemindahan rentas sempadan benar-benar diperlukan dalam pengendalian pemprosesan untuk mencapai tujuan yang dimaksudkan).

(c) **"Identify"**: Kenal pasti dan analisa risiko khusus terhadap perlindungan data peribadi bagi subjek data;

Penerangan

Ia mungkin melibatkan pertimbangan terhadap risiko pelanggaran mana-mana prinsip perlindungan data peribadi atau keperluan lain di bawah Akta 709 serta kesan yang mungkin berlaku kepada subjek data dan sebarang kemudaratan yang boleh timbul akibat pemprosesan, contohnya seperti:

- risiko keselamatan (termasuk punca risiko dan potensi impak bagi setiap jenis pelanggaran);
- ketidakupayaan untuk melaksanakan hak subjek data;
- kehilangan kawalan terhadap penggunaan data peribadi;
- pencurian identiti atau penipuan;
- kerugian kewangan;
- kecederaan fizikal;
- kehilangan kerahsiaan.
- negara di mana data dipindahkan mungkin tidak mempunyai undang-undang perlindungan data dan privasi yang mencukupi.

Tambahan lagi, analisis ke atas risiko khusus yang dikenal pasti harus mengambil kira kebarangkalian dan kemudaratan yang berpotensi. Matriks risiko (contoh seperti di bawah) boleh digunakan untuk menentukan tahap risiko bagi setiap risiko khusus yang dikenal pasti.

Contoh Matriks Risiko		**Kebarangkalian**		
		Rendah	**Sederhana**	**Berkemungkinan besar**
Kemudaratan	Impak minima	Risiko rendah	Risiko rendah	Risiko rendah
	Impak sederhana	Risiko rendah	Risiko sederhana	Risiko tinggi
	Kemudaratan serius	Risiko rendah	Risiko tinggi	Risiko tinggi

Sebagai ilustrasi, jika suatu pengendalian pemprosesan mempunyai risiko khusus seperti pencurian identiti, sesebuah organisasi harus mempertimbangkan:

- kebarangkalian (contohnya, adakah pencurian identiti pernah berlaku sebelum ini dalam organisasi tersebut atau di kalangan pesaing dalam industri yang sama atau kepada mana-mana pihak lain yang menggunakan pengendalian pemprosesan yang serupa); dan

- kemudaratan (contohnya, sejauh mana kemudaratan yang boleh berlaku berdasarkan seperti, jenis data peribadi yang terlibat dalam pengendalian pemprosesan (contohnya, nombor akaun bank), profil subjek data (contohnya, dewasa berbanding kanak-kanak),

untuk menentukan tahap risiko (contohnya, jika risiko pencurian identiti yang khusus berkemungkinan berlaku dan boleh menyebabkan kemudaratan serius kepada subjek data maka risiko ini dianggap sebagai risiko tinggi. Dalam kes ini, langkah-langkah lebih kukuh perlu diambil bagi menangani risiko tersebut pada langkah 4 dan/atau ia boleh mempengaruhi tahap risiko terhadap baki keseluruhan pada langkah 5.)

(d) "**Consider**": Pertimbangkan langkah-langkah yang perlu diambil untuk menangani risiko khusus yang dikenal pasti bagi memastikan perlindungan data peribadi terjaga;

Penerangan

Ini mungkin melibatkan satu atau lebih daripada langkah berikut:

- tidak mengumpul jenis data tertentu;

- mengurangkan kekerapan pemprosesan atau memendekkan tempoh penyimpanan data;

- melaksanakan langkah keselamatan tambahan untuk meningkatkan perlindungan data;

- menganonimkan *(anonymise)* atau mempseudonimkan *(pseudonymise)* data sensitif tertentu bagi mengurangkan risiko;

- menggunakan teknologi yang berbeza;

- memasukkan perlindungan kontrak tambahan dengan pihak ketiga yang terlibat dalam pemprosesan data;

- melaksanakan penilaian pemindahan data rentas sempadan untuk menentukan sama ada pemindahan tersebut dibenarkan di bawah Akta 709 dan/atau sama

ada negara penerima mempunyai undang-undang perlindungan data dan privasi yang mencukupi.

(e) "**Assess**": Menilai tahap risiko baki keseluruhan (contohnya, tinggi, sederhana, atau rendah) bagi pengendalian pemprosesan.

Penerangan

Ia mungkin melibatkan pertimbangan terhadap tahap risiko yang telah ditetapkan bagi setiap risiko khusus yang dikenal pasti serta langkah-langkah yang dicadangkan untuk menangani risiko tersebut bagi menentukan tahap risiko terhadap baki keseluruhan.

Soalan 4

Sila berikan justifikasi yang jelas untuk menyokong pandangan anda bagi soalan-soalan di bawah:

(a) Apakah pandangan anda mengenai pendekatan 5 langkah "DEICA" yang dicadangkan bagi pelaksanaan DPIA? Adakah ia mencukupi, atau terdapat aspek lain yang perlu dipertimbangkan?

(b) Apakah panduan khusus yang perlu dimasukkan ke dalam Garis Panduan DPIA bagi memastikan DPO dapat melaksanakan DPIA dengan lebih berkesan dan sistematik?

(c) Adakah terdapat keperluan untuk contoh praktikal atau templat disediakan untuk membantu pelaksanaan DPIA? Sekiranya ya, sila nyatakan.

[E] Pemberitahuan kepada Pesuruhjaya

2.16 **Latar Belakang**: Penyerahan DPIA kepada pengawal selia diperlukan di beberapa negara dan bidang kuasa, seperti:

(a) EU dan UK – jika terdapat risiko yang tinggi; dan

(b) Japan dan South Korea – dalam semua keadaan (walaupun hanya entiti kerajaan diwajibkan secara undang-undang untuk melaksanakan DPIA dalam keadaan tertentu).

2.17 Selain itu, di EU dan UK, pengawal data yang melaksanakan DPIA serta yang menentukan bahawa ia mempunyai risiko tinggi perlu berunding dengan pengawal selia sebelum pemprosesan serta mengemukakan maklumat berikut kepada pengawal selia:

(a) jika berkenaan, tanggungjawab berkenaan bagi pengawal data, pengawal data bersama dan pemproses data yang terlibat dalam pemprosesan khususnya bagi pemprosesan dalam kumpulan syarikat;

(b) tujuan dan kaedah pemprosesan yang dirancang;

(c) langkah dan perlindungan yang disediakan bagi melindungi hak dan kebebasan subjek data mengikut undang-undang;

(d) jika berkenaan, butiran perhubungan DPO; dan

(e) apa-apa maklumat lain yang diminta oleh pengawal selia.

2.18 **Cadangan**: Adalah dicadangkan bahawa jika **keseluruhan baki risiko dinilai sebagai tinggi**, pengawal data perlu **memaklumkan kepada Pesuruhjaya** mengenai DPIA yang telah dilaksanakan serta mengemukakan maklumat dan dokumen yang mungkin diperlukan oleh Pesuruhjaya. Namun, tiada keperluan untuk mendapatkan kelulusan atau berunding dengan Pesuruhjaya untuk meneruskan pengendalian pemprosesan data terlebih dahulu.

2.19 Dari segi medium pemberitahuan kepada Pesuruhjaya, dicadangkan supaya portal dalam talian (contohnya, https://daftar.pdp.gov.my/) disediakan, di mana DPO boleh memasukkan maklumat yang relevan serta memuat naik dokumen berkaitan ke dalam portal tersebut.

Soalan 5

Sila berikan justifikasi yang jelas untuk menyokong pandangan anda bagi soalan soalan di bawah:

(a) Apakah pandangan anda mengenai cadangan pada Perenggan 2.18 yang mewajibkan pengawal data untuk memaklumkan Pesuruhjaya sekiranya baki risiko keseluruhan dinilai sebagai tinggi?

(b) Adakah anda bersetuju bahawa pemberitahuan mengenai DPIA sahaja mencukupi tanpa keperluan untuk mendapatkan kelulusan atau rundingan dengan Pesuruhjaya?

(c) Apakah pandangan anda mengenai jenis maklumat dan dokumen yang perlu dikemukakan kepada Pesuruhjaya sebagai sebahagian daripada proses pemberitahuan?

(d) Apakah dokumen yang wajar disertakan untuk memastikan ketelusan dan pemantauan berkesan tanpa meletakkan beban pentadbiran yang berlebihan kepada pengawal data?

(e) Apakah pandangan anda mengenai cadangan pada Perenggan 2.19 untuk menyediakan portal dalam talian bagi proses pemberitahuan mengenai DPIA kepada Pesuruhjaya?

(f) Adakah pendekatan pada Perenggan 2.19 ini praktikal dan mencukupi atau adakah anda mencadangkan saluran alternatif untuk memastikan proses pemberitahuan mengenai DPIA lebih efisien dan mudah diakses?

[F] Apa yang perlu dilaksanakan selepas DPIA

2.20 **Latar belakang**: Selain pemberitahuan kepada pengawal selia, beberapa bidang kuasa telah menetapkan keperluan pasca-DPIA. Sebagai contoh, di Filipina, organisasi diwajibkan mengekalkan rekod lengkap berkaitan DPIA yang telah dilaksanakan.

2.21 **Cadangan**: Dicadangkan bahawa sekiranya pengawal data meneruskan pengendalian pemprosesan selepas menjalankan DPIA, mereka wajib melaksanakan **semua** perkara berikut:

(a) melaksanakan langkah-langkah mitigasi yang telah dicadangkan dalam DPIA untuk menguruskan risiko khusus yang telah dikenal pasti;

(b) memantau sebarang perkembangan yang boleh menjejaskan pengendalian pemprosesan dan risiko berkaitan (contohnya, perubahan dalam tujuan pemprosesan atau kelemahan baharu dalam teknologi) dari semasa ke semasa serta mengambil tindakan sewajarnya untuk menanganinya; dan

(c) menyimpan rekod lengkap semua DPIA yang dilaksanakan berserta dokumen berkaitan sekurang-kurangnya bagi tempoh dua (2) tahun dan memastikan ia tersedia untuk diserahkan kepada Pesuruhjaya jika diminta.

Soalan 6

Sila berikan justifikasi yang jelas untuk menyokong pandangan anda bagi soalan-soalan di bawah:

(a) Apakah pandangan anda mengenai keperluan pasca-DPIA yang dicadangkan?

(b) Apakah panduan khusus yang perlu dimasukkan ke dalam Garis Panduan DPIA bagi membantu DPO melaksanakan tanggungjawab mereka selepas menjalankan DPIA?

(c) Apakah pandangan anda mengenai tempoh penyimpanan sekurang-kurangnya dua (2) tahun bagi dokumentasi berkaitan DPIA?