# KERTAS KONSULTASI AWAM NO. 2/2025:

# GARIS PANDUAN MEREKA BENTUK BERDASARKAN PERLINDUNGAN DATA

**Tarikh Mula: 20 Mac 2025**

**Tarikh Tamat: 19 Mei 2025**

## BAHAGIAN 1: PENGENALAN DAN LATAR BELAKANG

1.1 Seksyen 5 Akta Perlindungan Data Peribadi 2010 ("**Akta 709**") menetapkan bahawa pemprosesan data peribadi oleh pengawal data hendaklah mematuhi Prinsip Perlindungan Data Peribadi[1] yang ditetapkan ("**Prinsip PDP**") ("**Keperluan Pematuhan Prinsip PDP**"). Akta Perlindungan Data Peribadi (Pindaan) 2024 telah mewajibkan pemproses data untuk mematuhi Prinsip Keselamatan seperti yang dinyatakan dalam Seksyen 9 di bawah Akta 709. Namun, tiada keperluan yang jelas yang mewajibkan pengawal data dan pemproses data untuk melaksanakan keperluan "mereka bentuk berdasarkan perlindungan data *(data protection by design)*" ("**DPbD**").

1.2 DPbD adalah konsep yang telah mantap dan telah diperuntukkan secara jelas dalam perundangan seperti Peraturan Perlindungan Data Umum Kesatuan Eropah ("**EU GDPR**") dan '*Philippines' National Privacy Commission Circular 2023-06 on Security of Personal Data'* ("**Surat Pekeliling NPC Filipina**"). Beberapa prinsip dalam konsep DPbD juga telah dimasukkan ke dalam undang-undang privasi data di seluruh dunia, termasuk Akta 709. Antara prinsip tersebut adalah:

(i) penentuan tujuan – tujuan pemprosesan data peribadi mesti dimaklumkan kepada subjek data pada atau sebelum data dikumpulkan *(prinsip notis dan pilihan);*

(ii) had penggunaan, penyimpanan, dan penzahiran – penggunaan, penyimpanan dan penzahiran data peribadi mesti dihadkan kepada tujuan yang dinyatakan kepada individu dan telah dipersetujui olehnya, kecuali jika dikehendaki oleh undang-undang (*prinsip am*)

(iii) keselamatan – langkah keselamatan mesti dilaksanakan bagi memastikan kerahsiaan, integriti, dan ketersediaan data peribadi secara berterusan, serta ketepatan data (*prinsip keselamatan*); dan

(iv) integriti data – data peribadi mestilah tepat, lengkap dan dikemas kini sejajar dengan keperluan bagi memenuhi tujuan yang dinyatakan (*prinsip integriti*).

Oleh itu, walaupun konsep DPbD tidak diperuntukkan secara eksplisit dalam Akta 709, prinsip prinsipnya secara asasnya dicerminkan dalam Prinsip PDP.

1.3 Penerapan pendekatan DPbD adalah penting dalam peralihan daripada perlindungan data yang bersifat reaktif kepada perlindungan data yang bersifat proaktif. Ia menggalakkan pengawal data untuk mengintegrasikan pertimbangan perlindungan data ke dalam semua aspek pengurusan data peribadi mereka **dari awal hingga akhir serta secara lalai *(by default)***. Pendekatan ini membantu pengawal data memastikan pematuhan yang berkesan terhadap Prinsip PDP dan memperkukuh perlindungan hak subjek data.

1.4 Bagi memastikan rangka perlindungan data peribadi Malaysia kekal relevan, berkesan dan selaras dengan landskap peraturan perlindungan data global, dicadangkan agar satu garis panduan ("**Garis Panduan DPbD**") diterbitkan bagi memberikan panduan tentang cara menerapkan pendekatan DPbD dalam pematuhan Prinsip PDP.

[1] Tujuh prinsip perlindungan data peribadi seperti yang dinyatakan dalam Seksyen 6 hingga 12 di bawah Akta 709.

1.5 Sehubungan itu, Kertas Konsultasi Awam ini ("**KKA**") bertujuan untuk mengumpulkan maklum balas orang awam mengenai aspek yang akan atau seharusnya dimasukkan dan dirangkumi dalam Garis Panduan DPbD.

## BAHAGIAN 2: KEPERLUAN DPBD YANG DICADANGKAN

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

(a) Definisi DPbD;

(b) Tujuh prinsip asas DPbD;

(c) Kaedah pelaksanaan DPbD dalam setiap Prinsip PDP; dan

(d) Perlindungan privasi kanak-kanak.

### [A] Definisi DPbD

2.2 **Latar Belakang:** DPbD ialah pendekatan yang mengintegrasikan langkah-langkah perlindungan data secara langsung ke dalam reka bentuk dan pembangunan projek, sistem, program, proses dan teknologi **dari awal** dan bukannya sesuatu pemikiran terkemudian. Ia memerlukan aspek privasi dipertimbangkan **pada setiap peringkat pemprosesan data**, daripada peringkat konsep awal, pembangunan, sehingga pelaksanaannya. Pendekatan ini menggalakkan perlindungan data **secara proaktif** dengan menekankan kepentingan untuk menjangka dan mencegah pelanggaran privasi, berbanding hanya bertindak balas selepas isu berkaitan perlindungan data berlaku.

**Contoh Pelaksanaan Sebenar DPbD**

Sebuah pasukan pemasaran menyimpan pangkalan data alamat e-mel yang dikumpulkan daripada pelanggan yang mendaftar untuk mendapatkan surat berita, membuat pesanan produk dan menghadiri pameran produk. Akta 709 menetapkan bahawa data peribadi mesti dipadamkan secara kekal apabila tidak lagi diperlukan untuk tujuan asal ianya dikumpulkan dan diproses (*prinsip penyimpanan*). Dalam usaha untuk mematuhi keperluan Akta 709 ini, pasukan tersebut kemudian mencipta pangkalan data pertanyaan bagi mengenal pasti tarikh alamat e-mel yang dikumpulkan dan menetapkan tempoh standard sebelum data tersebut dianggap tidak lagi diperlukan. Apabila alamat e-mel mencapai tempoh yang ditetapkan, ia akan ditandakan untuk semakan manual oleh pasukan bagi menentukan sama ada ia perlu dipadamkan.

Pendekatan ini mewujudkan kelemahan dalam perlindungan data—pasukan berdepan kesukaran untuk menjejaki bila dan untuk tujuan apa alamat e-mel dikumpulkan; selain itu, sesetengah data disimpan lebih lama daripada yang diperlukan kerana tempoh penyimpanan ditetapkan secara arbitrari.

Pendekatan DPbD yang lebih baik ialah merancang pangkalan data dari awal supaya setiap alamat e-mel diberikan tempoh penyimpanan yang ditetapkan secara automatik apabila ia dimasukkan ke dalam sistem. Setelah tempoh penyimpanan tamat, alamat e-mel boleh dipadamkan secara automatik atau sekurang-kurangnya disekat daripada digunakan sehingga ia disemak.

2.3 EU GDPR mentakrifkan DPbD seperti berikut:

**Artikel 25 EU GDPR**

*"Perlindungan Data berdasarkan reka bentuk (design) dan lalai (default)"*

*1. Dengan mengambil kira tahap perkembangan teknologi, kos pelaksanaan serta sifat, skop, konteks dan tujuan pemprosesan, serta risiko dengan tahap kemungkinan dan kesan yang berbeza terhadap hak dan kebebasan individu akibat pemprosesan tersebut, pengawal hendaklah, semasa menentukan kaedah pemprosesan dan semasa pemprosesan itu sendiri, melaksanakan langkah teknikal dan pengurusan yang sesuai seperti pseudonimisasi (pseudonymisation), yang direka untuk mengaplikasikan prinsip perlindungan data seperti pengurangan data (data minimisation), secara berkesan serta mengintegrasikan langkah perlindungan yang diperlukan ke dalam pemprosesan bagi memenuhi keperluan Peraturan ini dan melindungi hak subjek data.*

*2. Pengawal hendaklah melaksanakan langkah teknikal dan pengurusan yang sesuai bagi memastikan bahawa, secara lalai (by default) hanya data peribadi yang diperlukan untuk setiap tujuan pemprosesan tertentu diproses. Kewajipan ini terpakai kepada jumlah data peribadi yang dikumpulkan, skop pemprosesannya, tempoh penyimpanannya, dan kebolehcapaian. Secara khusus, langkah-langkah ini hendaklah memastikan bahawa secara lalai, data peribadi tidak boleh diakses oleh jumlah individu yang tidak ditentukan tanpa kebenaran subjek data.*

2.4 Dalam Surat Pekeliling NPC Filipina, DPbD ditakrifkan seperti berikut:

**Surat Pekeliling NPC Filipina**

*O.* ***"Mereka Bentuk Berdasarkan Privasi" (Privacy-by-Design)*** *merujuk kepada pendekatan dalam pembangunan dan pelaksanaan projek, program dan proses yang mengintegrasikan langkah perlindungan yang diperlukan ke dalam reka bentuk atau struktur bagi melindungi dan memelihara privasi dalam reka bentuk atau struktur sesuatu aktiviti pemprosesan atau sistem pemprosesan data.*

*P.* ***"Privasi Secara Lalai" (Privacy-by-Default)*** *merujuk kepada prinsip di mana Pengawal Maklumat Peribadi (PIC) atau Pemproses Maklumat Peribadi (PIP) memastikan bahawa hanya data yang diperlukan bagi setiap tujuan pemprosesan tertentu sahaja diproses secara lalai tanpa memerlukan campur tangan daripada subjek data.*

*7. PIC atau PIP hendaklah mengambil kira prinsip Mereka Bentuk Berdasarkan Privasi dalam aktiviti pemprosesannya dan memastikan Privasi Secara Lalai diterapkan dalam sistem pemprosesan data tanpa memerlukan sebarang tindakan daripada subjek data.*

*Selain itu, PIC atau PIP juga mesti menjalankan Penilaian Impak Privasi (PIA) terhadap perisian sedia ada, penyelesaian, atau sistem pemprosesan data seperti yang digariskan dalam Seksyen 5 Surat Pekeliling ini.*

*Sebarang fungsi yang tidak mempunyai asas undang-undang untuk pemprosesan atau tidak selaras dengan prinsip umum perlindungan data peribadi mesti dinyahaktifkan atau dimatikan.*

*8. PIC atau PIP hendaklah mengintegrasikan keperluan perlindungan data peribadi dalam setiap peringkat pembangunan dan pelaksanaan sistem pemprosesan data."*

2.5 **Cadangan**: Adalah dicadangkan agar DPbD ditakrifkan sebagai:

Mereka bentuk berdasarkan perlindungan data merujuk kepada pendekatan yang menggabungkan langkah-langkah teknikal dan pengurusan yang sesuai yang direka untuk melaksanakan Prinsip Perlindungan Data Peribadi ke dalam keseluruhan kitaran hayat sesuatu aktiviti pemprosesan, bermula daripada peringkat reka bentuk, pembangunan, pelaksanaan sehingga ke peringkat pelucutan.

2.6 Cadangan definisi DPbD adalah bertujuan untuk:

(a) mengintegrasikan dan menghubungkan konsep DPbD dengan Keperluan Pematuhan Prinsip PDP bagi menyesuaikannya dengan rangka kawal selia di Malaysia serta memudahkan pemahaman konsep ini.

(b) tidak terlalu bersifat mengikat bagi membolehkan organisasi pelbagai saiz dan jenis dapat menyesuaikan pendekatan mereka dalam melaksanakan DPbD.

(c) mengguna pakai bahasa yang serupa dengan EU GDPR bagi membolehkan pendekatan seragam dalam amalan perlindungan data di peringkat global serta berdasarkan amalan dan duluan yang berguna yang telah dibangunkan di negara lain, termasuk EU.

***Soalan 1***

***(a) Apakah pandangan anda mengenai definisi DPbD yang dicadangkan? Adakah definisi tersebut terlalu luas atau terlalu mengikat?***

***(b) Apakah pandangan anda mengenai contoh yang dicadangkan?***

## [B] Tujuh Prinsip Asas DPbD

2.7 **Latar Belakang:** Terdapat tujuh prinsip asas[2] yang membimbing pengamalan praktikal DPbD. Prinsip-prinsip asas ini adalah:

(a) proaktif bukan reaktif; pencegahan bukan pemulihan;

(b) privasi sebagai tetapan lalai;

(c) privasi diterapkan dalam reka bentuk;

(d) keupayaan penuh – keuntungan bersama, bukan keuntungan satu pihak atas kerugian pihak lain;

(e) keselamatan menyeluruh – perlindungan sepanjang kitaran hayat;

(f) keterlihatan dan ketelusan – memastikan keterbukaan; dan

(g) menghormati privasi pengguna – memastikan pengguna sebagai keutamaan.

2.8 **Cadangan:** Adalah dicadangkan bahawa Garis Panduan DPbD akan merujuk kepada tujuh prinsip asas[3] DPbD sebagai rangka panduan bagi pelaksanaan DPbD serta menyediakan ilustrasi tentang cara mengoperasikan prinsip-prinsip asas ini secara praktikal. Walaubagaimanapun, prinsip asas dan ilustrasi ini berfungsi sebagai panduan, bukan keperluan wajib atau senarai yang terhad.

## [B.1] Prinsip 1 DPbD: Proaktif bukan reaktif; pencegahan bukan pemulihan

2.9 Prinsip 1 DPbD, **"proaktif bukan reaktif; pencegahan bukan pemulihan"**, menekankan keperluan untuk menjangka dan mencegah risiko privasi sebelum ia berlaku. Ia menggalakkan pembangunan proses yang secara aktif menghalang pelanggaran data, berbanding hanya bertindak balas selepas sesuatu pelanggaran berlaku. [4]

2.10 Pengawal data / pemproses data perlu memperakui dengan jelas bahawa perlindungan privasi adalah lebih berkesan apabila ianya diterapkan dari awal dan dikekalkan secara berterusan, berbanding dilaksanakan kemudian. Ini bermaksud:

(a) membuat komitmen yang jelas di peringkat tertinggi organisasi untuk menetapkan dan menguatkuasakan standard privasi yang tinggi.

(b) mewujudkan budaya privasi yang dikongsi oleh semua pihak berkepentingan dengan komitmen terhadap penambahbaikan yang berterusan.

[2] Sila rujuk https://www.ipc.on.ca/sites/default/files/legacy/2018/01/pbd.pdf.
[3] Berdasarkan kepada https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.
[4] Berdasarkan kepada https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

(c) membangunkan mekanisme untuk mengenal pasti kelemahan dalam reka bentuk privasi, menjangka amalan serta hasil privasi yang tidak memadai dan mengambil langkah pembetulan secara proaktif dan sistematik sebelum sebarang masalah timbul.

**Pelaksanaan prinsip "proaktif bukan reaktif; pencegahan bukan pemulihan"[5]**

- Memastikan kepimpinan tertinggi komited dan terlibat dalam membangunkan program privasi yang kukuh dan proaktif dalam organisasi, termasuk dengan:
    - memastikan terdapat individu yang mempunyai kepakaran dalam perlindungan data peribadi dalam lembaga pengarah serta memastikan pengarah menerima latihan yang sesuai mengenai perlindungan data peribadi.
    - memastikan pengarah memperuntukkan sumber yang mencukupi untuk program perlindungan data peribadi.
    - melantik sekurang-kurangnya seorang pengurus kanan yang bertanggungjawab terhadap pematuhan perlindungan data peribadi organisasi.
    - mengintegrasikan pematuhan perlindungan data peribadi sebagai sebahagian daripada penilaian prestasi dan ganjaran pengurusan kanan.
    - mewajibkan penilaian dan audit perlindungan data peribadi dilakukan serta dilaporkan kepada lembaga pengarah secara berkala.
    - mengemukakan soalan yang tepat kepada pengurusan kanan mengenai amalan perlindungan data peribadi dalam organisasi.
- Melaksanakan audit berkala terhadap dasar perlindungan data peribadi untuk memastikan keberkesanannya dalam pelaksanaan sebenar.
- Membangunkan kaedah sistematik, termasuk penilaian impak perlindungan data peribadi, bagi mengenal pasti dan menilai risiko serta membetulkan sebarang kelemahan sebelum ia mengakibatkan kesan negatif.
- Membudayakan persekitaran yang menggalakkan semua pihak berkepentingan termasuk pengguna untuk mencadangkan penambahbaikan terhadap amalan perlindungan data peribadi dengan memastikan setiap cadangan dikaji secara sistematik dan dilaksanakan apabila bersesuaian.

[5] Berdasarkan kepada https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.

***Soalan 2***

***Apakah pandangan anda mengenai penerapan Prinsip 1 DPbD sebagai salah satu prinsip asas dalam pelaksanaan DPbD?***

## [B.2] Prinsip 2 DPbD: Privasi sebagai tetapan lalai

2.11 Prinsip 2 DPbD, **"privasi sebagai tetapan lalai"**, menekankan bahawa data peribadi mesti dilindungi secara automatik dalam setiap sistem.[6] Ini bermaksud, **walaupun seseorang individu tidak mengambil sebarang tindakan, privasi mereka tetap terpelihara**. Tiada tindakan tambahan diperlukan daripada individu tersebut untuk melindungi privasi mereka kerana ia telah diterapkan secara lalai dalam sistem. Pendekatan privasi secara lalai ini boleh diringkaskan kepada amalan utama berikut:

(a) **Penentuan tujuan:** Tujuan pengumpulan, penggunaan, penyimpanan dan penzahiran data peribadi mesti dimaklumkan kepada subjek data pada atau sebelum maklumat tersebut dikumpulkan. Tujuan yang dinyatakan mestilah jelas, terhad dan relevan dengan keadaan yang khusus.

(b) **Had pengumpulan:** Pengumpulan data peribadi mesti dilakukan secara sah dan dihadkan kepada maklumat yang benar-benar diperlukan bagi tujuan yang telah ditetapkan.

(c) **Pengurangan data:** Pengumpulan data peribadi mesti dikekalkan pada tahap minimum yang ketat. Reka bentuk program, teknologi maklumat dan komunikasi serta sistem harus bermula dengan interaksi dan transaksi yang tidak boleh dikenal pasti sebagai tetapan lalai. Seboleh mungkin, kebolehkenalan, kebolehamatan dan kebolehhubungan (keupayaan data untuk dikaitkan) terhadap data peribadi harus diminimumkan.

(d) **Had penggunaan, penyimpanan dan penzahiran:** Penggunaan, penyimpanan dan penzahiran data peribadi mesti dihadkan kepada tujuan yang telah dimaklumkan kepada individu dan dipersetujui olehnya, kecuali jika dikehendaki selainnya oleh undang-undang. Data peribadi mesti disimpan hanya selama mana ia diperlukan untuk memenuhi tujuan yang dinyatakan dan kemudian dimusnahkan dengan selamat.

(e) **Jika keperluan atau tujuan penggunaan data peribadi tidak jelas, prinsip privasi hendaklah diutamakan dan pendekatan berwaspada mesti diterapkan:** tetapan lalai mestilah memastikan perlindungan privasi yang maksimum.

[6] Berdasarkan kepada https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

**Pelaksanaan Prinsip "Privasi sebagai Tetapan Lalai"** [7]

- Mulakan tanpa pengumpulan data peribadi kecuali dan sehingga terdapat tujuan yang jelas dan kukuh untuk pengumpulan data tersebut. Tetapkan tujuan pengumpulan data peribadi sejelas dan sesempit mungkin. Gunakan sistem persetujuan aktif *(opt-in)*.

- Minimakan pengumpulan data daripada awal, hanya kepada maklumat yang benar-benar diperlukan untuk tujuan yang telah dikenal pasti.

- Hadkan penggunaan dan penyimpanan data peribadi hanya bagi tujuan khusus yang dinyatakan semasa data dikumpulkan.

- Wujudkan halangan teknologi, dasar dan prosedur yang menghubungkan data peribadi. Contohnya, asingkan data peribadi yang diproses untuk tujuan berbeza dalam pangkalan data atau sistem berasingan secara lalai bagi mengelakkan pertukaran data yang tidak diperlukan. Ini termasuk melaksanakan kawalan akses supaya hanya individu yang benar-benar memerlukan akses kepada data dibenarkan mengaksesnya. Bagi platform dalam talian, elakkan profil pengguna dilihat awam melainkan pengguna mengambil langkah nyata untuk membenarkannya.

***Soalan 3***

***Apakah pandangan anda mengenai penerapan Prinsip 2 DPbD sebagai salah satu prinsip asas dalam pelaksanaan DPbD?***

## [B.3] Prinsip 3 DPbD: Privasi Diterapkan dalam Reka Bentuk

2.12 Prinsip 3 DPbD , **"privasi diterapkan dalam reka bentuk"**, menekankan pengintegrasian privasi secara menyeluruh ke dalam teknologi, operasi dan seni bina maklumat dengan cara yang bersepadu dan inovatif. [8] Ia melibatkan:

(a) menerapkan privasi secara sistematik dan berasaskan prinsip – menggunakan piawaian serta rangka tetap yang membolehkan semakan dan audit bebas serta memastikan Prinsip PDP diterapkan secara konsisten dalam keseluruhan proses reka bentuk dan operasi.

(b) melaksanakan penilaian impak perlindungan data secara menyeluruh dengan mendokumentasikan risiko privasi secara jelas serta semua langkah mitigasi yang diambil termasuk menilai alternatif lain bagi mengurangkan risiko tersebut; dan

[7] Berdasarkan kepada https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.
[8] Berdasarkan kepada https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

(c) memastikan perlindungan data peribadi direka bentuk untuk mengurangkan risiko privasi secara maksimum agar tidak mudah terdedah kepada kelemahan akibat penggunaan, salah konfigurasi atau kesilapan manusia.

**Contoh praktikal "mereka bentuk berdasarkan privasi"**

Sebuah peruncit fesyen bercadang untuk melancarkan kedai dalam talian bagi menjual pakaian dan aksesori kepada pelanggan. Sejak awal pembangunan laman web, pasukan reka bentuk telah menetapkan privasi sebagai salah satu objektif utama laman web tersebut. Pasukan ini menjalankan penilaian menyeluruh terhadap kaedah pembangunan dan reka bentuk web bagi memilih rangka yang menawarkan ciri privasi yang dipertingkatkan serta memastikan laman web mematuhi piawaian sistem keselamatan maklumat yang telah ditetapkan.

Sistem pangkalan data khusus dengan protokol penyulitan berlapis digunakan bagi menyimpan dan memproses data peribadi pelanggan dengan selamat. Sistem pengurusan identiti yang mengutamakan pengguna diterapkan untuk menyediakan pengalaman pengguna yang lancar merentasi pelbagai peranti dengan notis perlindungan data peribadi yang mudah diakses serta ciri-ciri dalaman terbina yang membolehkan pengguna mengakses, memadam dan membetulkan data peribadi mereka dengan mudah.

Sebelum melancarkan kedai dalam talian, pasukan tersebut menjalankan penilaian impak perlindungan data terhadap infrastruktur IT bagi mengenal pasti sebarang risiko privasi. Langkah mitigasi dilaksanakan untuk menangani risiko yang dikenalpasti. Audit dan penilaian berkala dijalankan selepas pelancaran bagi memastikan keberkesanan berterusan ciri perlindungan privasi yang diterapkan.

***Soalan 4***

***Apakah pandangan anda mengenai penerapan Prinsip 3 DPbD sebagai salah satu prinsip asas dalam pelaksanaan DPbD?***

## [B.4] Prinsip 4 DPbD: Keupayaan penuh – keuntungan bersama, bukan keuntungan satu pihak atas kerugian pihak lain

2.13 Prinsip 4 DPbD, **"keupayaan penuh – keuntungan bersama, bukan keuntungan satu pihak atas kerugian pihak lain"** menekankan keperluan untuk menampung semua kepentingan dan objektif yang sah dengan cara yang memberikan manfaat kepada semua pihak berkepentingan tanpa perlu mengorbankan privasi secara tidak perlu. [9] Ia menolak tanggapan salah bahawa privasi tidak boleh wujud seiring dengan kepentingan perniagaan yang sah. Ini bermaksud:

[9] Berdasarkan kepada https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

(a) apabila menerapkan privasi dalam sesuatu teknologi, proses atau sistem, ia harus dilakukan dengan cara yang tidak menjejaskan keupayaan penuh serta memastikan semua keperluan dioptimumkan semaksimum mungkin.

(b) semua kepentingan dan objektif, fungsi yang diinginkan serta metrik yang digunakan harus dinyatakan dengan jelas, didokumentasikan, dipersetujui dan diterapkan. Sebarang kompromi harus ditolak dengan keutamaan diberikan kepada penyelesaian yang membolehkan pelbagai fungsi beroperasi secara serentak.

**Pelaksanaan Praktikal Prinsip "Keupayaan Penuh – Keuntungan Bersama, Bukan Keuntungan Satu Pihak atas Kerugian Pihak Lain"** [10]

- Mengakui bahawa pelbagai kepentingan perniagaan yang sah boleh wujud secara serentak tanpa perlu mengorbankan privasi.

- Melibatkan komunikasi, perundingan dan kerjasama untuk memahami pelbagai kepentingan yang mungkin bertentangan pada masa tertentu.

- Mencari penyelesaian inovatif dan pilihan alternatif bagi mencapai pelbagai fungsi secara serentak tanpa perlu berkompromi terhadap privasi.

**Contoh praktikal "keupayaan penuh – keuntungan bersama, bukan keuntungan satu pihak atas kerugian pihak lain"** [11]

Sebuah bangunan sedang menaik taraf sistem pemantauan videonya yang lama bagi meningkatkan kecekapan dan keselamatan. Sistem lama bergantung sepenuhnya kepada kakitangan keselamatan yang perlu memantau sejumlah besar skrin video secara langsung untuk mengesan penceroboh dan memantau kawasan terhad secara manual.

Bagi mencapai objektif privasi, kecekapan dan keselamatan secara serentak, sistem pemantauan video yang baharu menggabungkan dua mod operasi:

(i) mod operasi lalai yang kurang mengganggu privasi untuk pengesanan pencerobohan di kawasan terhad; dan

(ii) mod amaran yang lebih invasif untuk menjejaki dan mengenal pasti lokasi penceroboh.

Dalam mod lalai, sistem ini menjalankan pengesanan pencerobohan dengan tahap gangguan privasi yang minimum. Algoritma pengesanan dan penjejakan manusia hanya beroperasi pada kamera tertentu yang meliputi kawasan terhad dan strim video daripada kamera tersebut tidak dipaparkan kepada pengendali. Tiada data peribadi direkodkan dalam mod lalai ini. Hanya apabila penceroboh dikesan, sistem secara automatik beralih ke mod amaran, yang mengaktifkan penjejakan penceroboh dan memulakan rakaman video kamera.

[10] Berdasarkan kepada https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.
[11] Berdasarkan kepada https://www.researchgate.net/publication/284780818_How_Is_Positive-Sum_Privacy_Feasible.

***Soalan 5***

***Apakah pandangan anda mengenai penerapan Prinsip 4 DPbD sebagai salah satu prinsip asas dalam pelaksanaan DPbD?***

## [B.5] Prinsip 5 DPbD: Keselamatan Menyeluruh – Perlindungan Sepanjang Kitaran Hayat

2.14 Prinsip 5 DPbD, **"keselamatan menyeluruh – perlindungan sepanjang kitaran hayat"**, menekankan kepentingan memastikan keselamatan data di sepanjang keseluruhan kitaran hayat data peribadi. Semua data mesti disimpan dengan selamat dan dimusnahkan secara selamat setelah proses berakhir, dalam tempoh yang sesuai. Sepatutnya tiada jurang dalam perlindungan atau akauntabiliti. Ini bermaksud:

(b) mengambil tanggungjawab penuh terhadap keselamatan data peribadi sepanjang kitaran hayatnya, berdasarkan tahap sensitiviti data dan selaras dengan piawaian keselamatan data yang ditetapkan; dan

(c) antara lain, melaksanakan kaedah pemusnahan selamat, penyulitan yang sesuai dan kawalan akses serta kaedah log yang kukuh bagi memastikan kerahsiaan, integriti dan ketersediaan data peribadi sepanjang kitaran hayatnya.

**Pelaksanaan Praktikal Prinsip "Keselamatan Menyeluruh – Perlindungan Sepanjang Kitaran Hayat"** [12]

Sebuah peruncit e-dagang menggunakan teknologi penyulitan Transport Layer Security (TLS) (protokol kriptografi) bagi melindungi data yang dimasukkan oleh pelanggan semasa proses pembayaran untuk memastikan keselamatan data sepanjang penghantaran.

Data yang disimpan dalam pangkalan data peruncit dilindungi dengan penyulitan Advanced Encryption Standard (AES)-256, dengan kunci penyulitan dikendalikan secara selamat dalam sistem pengurusan kunci khusus. Sandar data yang disulitkan *(encrypted backup)* secara automatik memastikan integriti data terpelihara, manakala rancangan pemulihan bencana yang komprehensif disediakan untuk memulihkan operasi dengan cepat dan mendapatkan kembali data pelanggan sekiranya berlaku pelanggaran data atau kegagalan sistem.

API yang selamat dan penyulitan hujung-ke-hujung *(end-to-end encryption)* digunakan bagi memastikan keselamatan data yang dihantar antara sistem peruncit dan rakan kongsi luaran seperti pemproses pembayaran dan penyedia perkhidmatan logistik.

Untuk kawalan akses dalaman, kakitangan perlu menggunakan pengesahan pelbagai faktor (multi-factor authentication) untuk log masuk ke platform e-dagang. Kawalan akses berasaskan peranan

[12] Berdasarkan kepada https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.

diterapkan bagi memastikan hanya kakitangan yang diberi kuasa boleh mengakses data tertentu -- wakil jualan hanya mempunyai akses kepada pesanan pelanggan yang ditugaskan kepada mereka untuk memberikan perkhidmatan pelanggan yang diperibadikan. Pengurus inventori hanya boleh mengakses data stok untuk memantau ketersediaan produk. Pengurus pemasaran hanya mempunyai akses kepada data demografi pelanggan, corak pembelian serta analitik prestasi kempen untuk mengoptimumkan strategi pemasaran dan promosi. Bagi memastikan privasi pelanggan dipelihara, peruncit menggunakan teknik anonimisasi *(anonymization)* dan pengagregatan data dalam analitik pemasaran bagi melindungi identiti pelanggan sambil tetap memperoleh maklumat yang bermakna. Langkah perlindungan titik akhir *(endpoint protection)* turut dilaksanakan untuk menjamin keselamatan peranti yang mengakses data pelanggan. Kakitangan menjalani latihan berterusan mengenai amalan terbaik dalam privasi dan keselamatan data bagi mengurangkan risiko pelanggaran akibat kesilapan manusia.

Dasar penyimpanan data yang jelas ditetapkan bagi menentukan tempoh penyimpanan data pelanggan. Apabila tempoh penyimpanan yang ditetapkan tamat, kaedah pemadaman selamat digunakan bagi memadam data pelanggan secara menyeluruh untuk mengelakkan akses yang tidak dibenarkan atau penyalahgunaan data di masa hadapan.

***Soalan 6***

***Apakah pandangan anda mengenai penerapan Prinsip 5 DPbD sebagai salah satu prinsip asas dalam pelaksanaan DPbD?***

## [B.6] Prinsip 6 DPbD: Keterlihatan dan ketelusan – memastikan keterbukaan

2.15 Prinsip 6 DPbD, **"keterlihatan dan ketelusan – memastikan keterbukaan"**, menekankan kepentingan menunjukkan akauntabiliti dalam aktiviti pemprosesan data peribadi. Data peribadi harus dikendalikan selaras dengan komitmen dan objektif yang telah dinyatakan, serta tertakluk kepada pengesahan bebas. Ini melibatkan:

(a) **Akauntabiliti**: Pengumpulan data peribadi melibatkan tanggungjawab untuk melindunginya. Semua dasar dan prosedur berkaitan privasi harus didokumentasikan dan dikomunikasikan dengan sewajarnya serta ditugaskan kepada individu tertentu. Apabila data peribadi dipindahkan kepada pihak ketiga, pastikan perlindungan data peribadi yang setara diterapkan melalui perjanjian kontrak atau kaedah lain;

(b) **Keterbukaan**: Keterbukaan dan ketelusan adalah elemen utama dalam memastikan akauntabiliti. Maklumat mengenai dasar dan amalan berkaitan pengurusan data peribadi harus tersedia dengan mudah kepada individu; dan

(c) **Pematuhan**: Mekanisme aduan dan penyelesaian perlu diwujudkan serta dikomunikasikan dengan jelas kepada individu, termasuk prosedur untuk mengemukakan aduan. Langkah-

langkah pemantauan, penilaian dan pengesahan pematuhan terhadap dasar serta prosedur perlindungan data peribadi harus dilaksanakan.

**Contoh praktikal "keterlihatan dan ketelusan – memastikan keterbukaan"**

Sebuah platform e-dagang menyampaikan notis perlindungan data peribadi tepat pada masanya atau '*just-in-time*' apabila pelanggan diminta untuk memberikan data peribadi mereka, seperti semasa mencipta akaun pengguna atau membuat pesanan. Notis tersebut ditulis dalam bahasa yang jelas dan ringkas serta disusun secara berlapis (layered format), di mana maklumat utama ditegaskan menggunakan saiz dan gaya fon *(font)* yang berbeza dan pautan diberikan bagi maklumat yang lebih terperinci. Selain itu, notis perlindungan data peribadi dalam bentuk tetingkap makluman atau '*pop-up*' turut dipaparkan pada platform bagi memaklumkan pelanggan mengenai data peribadi yang dikumpulkan secara automatik, seperti kuki, suar web (web beacons), skrip penjejakan dan aplikasi lain yang digunakan oleh platform tersebut. Di setiap halaman web platform, terdapat pautan yang mudah dilihat dan diakses ke notis perlindungan data peribadi yang lebih menyeluruh.

***Soalan 7***

***Apakah pandangan anda mengenai penerapan Prinsip 6 DPbD sebagai salah satu prinsip asas dalam pelaksanaan DPbD?***

## [B.7] Prinsip 7 DPbD: Menghormati privasi pengguna – memastikan pengguna sebagai keutamaan

2.16 Prinsip 7 DPbD, **"menghormati privasi pengguna – memastikan pengguna sebagai keutamaan"**, menekankan kepentingan mengutamakan kepentingan individu dengan menyediakan langkah-langkah seperti tetapan privasi yang kukuh secara lalai, notis yang sesuai dan memberi pilihan yang mesra pengguna.

2.17 Projek, produk, perkhidmatan, sistem dan proses harus dirancang dengan mengambil kira kepentingan dan keperluan pengguna individu kerana merekalah pihak yang mempunyai kepentingan terbesar dalam pengurusan data peribadi mereka sendiri. Ia melibatkan:

(a) **Persetujuan:** Persetujuan individu yang diberikan secara bebas dan khusus diperlukan bagi tujuan pengumpulan, penggunaan atau penzahiran data peribadi kecuali jika dibenarkan sebaliknya oleh undang-undang. Semakin sensitif data tersebut, semakin jelas dan khusus persetujuan yang diperlukan. Persetujuan boleh ditarik balik pada masa akan datang.

(b) **Ketepatan:** Data peribadi mestilah tepat, lengkap dan dikemas kini setakat yang diperlukan untuk memenuhi tujuan yang telah dinyatakan.

(c) **Akses:** Individu patut diberikan akses kepada data peribadi mereka serta dimaklumkan mengenai bagaimana data mereka digunakan dan kepada siapa ia didedahkan. Mereka juga mesti mempunyai hak untuk mencabar ketepatan dan kelengkapan data mereka serta meminta pembetulan dibuat jika perlu.

(d) **Pematuhan:** Organisasi wajar mewujudkkan mekasime aduan dan pembetulan *(redress)* serta menghebahkan maklumat mengenainya kepada orang ramai termasuk cara untuk membawa aduan ke peringkat rayuan seterusnya jika perlu.

**Contoh praktikal "menghormati privasi pengguna – memastikan pengguna sebagai keutamaan"**

Sebuah aplikasi mudah alih berkaitan kecergasan memberikan pengguna kawalan penuh ke atas maklumat peribadi yang mereka kongsi semasa mencipta atau mengemas kini profil mereka, dengan pilihan yang jelas dan mudah difahami. Aplikasi ini menggunakan persetujuan berasingan bagi setiap tujuan pemprosesan data, membolehkan pengguna menentukan akses kepada maklumat tertentu seperti jantina, status hubungan, lokasi, sejarah kecergasan dan lain-lain. Selain itu, aplikasi ini dilengkapi dengan papan pemuka privasi yang memberikan gambaran menyeluruh mengenai data yang dikumpulkan serta cara ia digunakan. Pengguna juga boleh menyesuaikan keutamaan perlindungan data mereka, termasuk memilih sama ada untuk berkongsi data bagi tujuan analisis atau menerima cadangan kandungan yang diperibadikan. Untuk memastikan ketelusan, notifikasi dalam aplikasi akan memaklumkan pengguna tentang sebarang perubahan pada dasar perlindungan data peribadi secara tepat pada masanya, membolehkan mereka memahami dan membuat keputusan sebelum perubahan tersebut memberi kesan kepada data peribadi mereka.

***Soalan 8***

***Apakah pandangan anda mengenai penerapan Prinsip 7 DPbD sebagai salah satu prinsip asas dalam pelaksanaan DPbD?***

## [C] Cara Melaksanakan DPbD dalam Setiap Prinsip PDP

2.18 **Latar Belakang:** Garis Panduan EU 4/2019 mengenai Perkara 25 Mereka Bentuk dan Lalai Berdasarkan Perlindungan ("**Garis Panduan EU**") telah dikeluarkan oleh Lembaga Perlindungan Data Eropah (EDPB) pada tahun 2020 untuk memberikan panduan mengenai tafsiran kewajipan DPbD di bawah Perkara 25 GDPR. Garis panduan ini merangkumi contoh elemen reka bentuk dan tetapan lalai bagi setiap prinsip perlindungan data serta cadangan bagaimana pengawal, pemproses dan pengeluar boleh bekerjasama untuk mencapai pematuhan DPbD.

2.19 **Cadangan:** Selaras dengan pendekatan di EU, adalah dicadangkan bahawa Garis Panduan DPbD akan menerangkan serta memberikan contoh praktikal mengenai cara melaksanakan DPbD bagi **tujuh Prinsip PDP** di bawah Akta 709, seperti yang diterapkan di EU.

2.20 Garis panduan ini akan menggariskan elemen utama untuk mengoperasikan DPbD bagi **setiap Prinsip PDP** dengan merujuk kepada amalan dan panduan daripada Garis Panduan EU.

## [C.1] Prinsip Am

2.21 **Prinsip am**[13] mengkehendaki pengawal data untuk:

(a) mengenal pasti asas undang-undang yang sah bagi pemprosesan data peribadi;

(b) memproses data peribadi hanya untuk tujuan yang sah dan berkaitan secara langsung dengan aktiviti pengawal data; dan

(c) hanya memproses data peribadi yang mencukupi, relevan dan terhad kepada apa yang diperlukan bagi tujuan tersebut.

2.22 Pengawal data harus membentuk reka bentuk operasi pemprosesan data berdasarkan keperluan untuk mencapai tujuan pemprosesan. Langkah-langkah kawalan dan perlindungan perlu dilaksanakan bagi memastikan keseluruhan kitaran pemprosesan data mematuhi asas undang-undang yang berkaitan serta tujuan pemprosesan.

2.23 Elemen utama DPbD bagi prinsip Ini termasuk:

(a) **Pengurangan data:** Pengawal data harus terlebih dahulu menentukan sama ada mereka benar-benar perlu memproses data peribadi untuk tujuan yang relevan. Pengawal data harus mengesahkan sama ada tujuan yang berkaitan boleh dicapai dengan memproses bilangan data peribadi yang lebih minima, menggunakan data yang kurang terperinci atau dalam bentuk agregat atau tanpa perlu memproses data peribadi sama sekali. Pengesahan ini harus dilakukan sebelum sebarang pemprosesan dijalankan.

Pengurangan data juga boleh merujuk kepada tahap pengecaman. Jika tujuan pemprosesan tidak memerlukan set data akhir merujuk kepada individu yang dikenal pasti atau boleh dikenal pasti (seperti dalam statistik), tetapi pemprosesan awal memerlukannya (contohnya sebelum data diagregatkan), **maka pengawal data harus memadam atau menganonimkan data peribadi sebaik sahaja pengecaman tidak lagi diperlukan**. Atau, jika pengecaman berterusan diperlukan untuk aktiviti pemprosesan lain, data peribadi harus dipseduonimkan *(pseudonymized)* untuk mengurangkan risiko terhadap hak subjek data.

(b) **Penentuan awal:** Tujuan dan asas undang-undang bagi pemprosesan harus ditetapkan sebelum **pemprosesan** dijalankan. Prinsip ini seharusnya mempengaruhi reka bentuk pemprosesan dan menetapkan had pemprosesan.

[13] Akta 709, s. 6.

(c) **Kekhususan**: Tujuan pemprosesan harus dinyatakan dengan jelas dan spesifik.

(d) **Pengelakan data**: Pengawal data harus mengelakkan pemprosesan data peribadi sepenuhnya jika tujuan yang berkaitan dapat dicapai tanpa pemprosesan. Data yang diagregatkan harus digunakan jika boleh.

(e) **Pembezaan:** Asas undang-undang dan tujuan yang digunakan untuk setiap aktiviti pemprosesan harus dibezakan.

(f) **Keberkaitan**: Asas undang-undang yang digunakan dalam pemprosesan mestilah tepat dan berkait secara langsung dengan tujuan pemprosesan. Data peribadi yang diproses haruslah relevan, bersesuaian serta diperlukan untuk tujuan tersebut dan Pengawal data wajar membuktikan kaitan tersebut.

(g) **Keperluan:** Hanya data peribadi yang benar-benar diperlukan untuk memenuhi tujuan pemprosesan boleh dikumpulkan dan diproses. Setiap kategori data peribadi haruslah mempunyai justifikasi yang kukuh dan hanya boleh diproses jika tiada alternatif lain yang boleh mencapai tujuan tersebut.

(h) **Had:** Pengawal data harus mengehadkan pengumpulan data peribadi kepada jumlah minimum yang diperlukan untuk tujuan yang dinyatakan. Tiada pemprosesan tambahan wajar dilakukan untuk tujuan lain di luar skop asal pengumpulan data. Langkah teknikal seperti penceraian data dan penyulitan serta langkah pengurusan seperti dasar dalaman dan kewajipan kontrak harus dilaksanakan bagi mencegah penyalahgunaan atau penggunaan semula data peribadi untuk tujuan lain.

(i) **Semakan:** Semakan berkala harus dijalankan untuk memastikan pemprosesan data masih diperlukan bagi tujuan asal.

(j) **Penamatan:** Jika asas undang-undang atau tujuan pemprosesan tidak lagi terpakai, pemprosesan data mesti dihentikan serta-merta bagi memastikan pematuhan terhadap keperluan perlindungan data.

(k) **Pelarasan:** Jika terdapat perubahan yang sah dalam asas undang-undang bagi pemprosesan, pemprosesan data mesti diselaraskan mengikut asas undang-undang yang baharu bagi memastikan pematuhan terhadap peraturan yang berkuat kuasa.

(l) **Pembahagian tanggungjawab:** Jika lebih daripada satu pengawal data terlibat dalam pemprosesan, setiap pihak mesti memperjelaskan dan memperuntukkan tanggungjawab mereka secara telus terhadap subjek data. Reka bentuk pemprosesan harus dirancang dengan jelas mengikut pembahagian tanggungjawab yang dipersetujui.

(m) **Teknologi pemerkasaan privasi:** Pengawal data disarankan untuk menggunakan teknologi yang terkini dan sesuai bagi tujuan pengelakan dan pengurangan data.

(n) **Persetujuan:** Jika persetujuan digunakan sebagai asas undang-undang bagi pemprosesan data, pengawal data mesti memastikan bahawa persetujuan diberikan secara bebas, khusus, dimaklumkan dan jelas. Mekanisme yang mudah harus disediakan bagi membolehkan subjek data menarik balik persetujuan mereka dengan cara yang sama mudah seperti pemberian persetujuan.

**Contoh Praktikal Pelaksanaan DPbD bagi Prinsip Am** [14]

Sebuah kafe bercadang untuk melancarkan sistem pesanan dalam talian berserta program kesetiaan pelanggan yang membolehkan pelanggan membuat pesanan lebih awal, mengambil pesanan mereka dan menikmati faedah keahlian tertentu. Sebelum melancarkan sistem tersebut, kafe ini menyenaraikan sebab-sebab mengapa terdapat keperluan untuk mendapatkan data peribadi pelanggan, iaitu bagi tujuan:

- memproses pesanan
- memproses pembayaran
- memberitahu pelanggan apabila pesanan mereka sedia untuk diambil
- mengesahkan pelanggan yang betul sedang mengambil pesanan
- membolehkan ahli menikmati faedah keahlian, termasuk ganjaran hari lahir
- mengumpul maklum balas daripada pelanggan untuk meningkatkan perkhidmatan
- menghantar e-mel pemasaran kepada pelanggan mengenai produk baharu dan promosi

Kafe ini mengenal pasti jenis data peribadi pelanggan yang dikumpulkan dan mengesahkan sama ada setiap jenis data peribadi benar-benar diperlukan bagi tujuan pemprosesan. Sebagai contoh, kafe tersebut mendapati bahawa pelanggan tidak perlu membuka akaun untuk membuat pesanan. Setiap pesanan yang berjaya akan menjana kod unik secara automatik, yang boleh digunakan pelanggan untuk mengenal pasti diri mereka semasa mengambil pesanan. Oleh itu, kafe hanya mengumpulkan data peribadi yang minimum untuk pelanggan membuat pesanan, iaitu nama pertama dan alamat e-mel sekiranya pelanggan gagal mencatat kod unik tersebut. Selain itu, kafe tersebut turut mendapati meskipun borang keahlian mengumpulkan tarikh lahir pelanggan, termasuk hari, bulan dan tahun bagi tujuan penebusan ganjaran hari lahir, namun ia menyedari bahawa tahun lahir sebenarnya tidak diperlukan untuk tujuan tersebut, maka data tersebut tidak perlu dikumpulkan.

Kafe tersebut seterusnya mengenal pasti asas undang-undang yang boleh digunakan bagi setiap tujuan pemprosesan.

[14] Based on https://ethyca.com/blog/data-minimization-a-privacy-engineers-guide-on-getting-started.

| *Asas undang-undang* | *Tujuan* |
|---|---|
| Pelaksanaan kontrak yang melibatkan subjek data | ● Memproses pesanan<br>● Memproses pembayaran<br>● Memberitahu pelanggan apabila pesanan mereka sedia untuk diambil<br>● Mengesahkan pelanggan yang betul sedang mengambil pesanan<br>● Membolehkan ahli menikmati faedah keahlian, termasuk ganjaran hari lahir |
| Persetujuan | ● Mengumpul maklum balas daripada pelanggan untuk meningkatkan perkhidmatan<br>● Menghantar e-mel pemasaran kepada pelanggan mengenai produk baharu dan promosi |

Kafe ini memastikan bahawa persetujuan yang berasingan dan khusus diperoleh semasa mengumpul data peribadi pelanggan bagi tujuan mengumpulkan maklum balas tentang perkhidmatannya dan menghantar e-mel pemasaran kepada pelanggan. Pelanggan diberikan pilihan untuk bersetuju dengan menerima e-mel pemasaran dengan menandakan kotak semak semasa membuat pesanan. Secara lalai, kotak semak ini tidak ditandakan.

Pelanggan yang memberikan maklum balas melalui borang maklum balas dalam talian di laman web secara jelas diingatkan supaya berhati-hati dalam menyertakan data peribadi mereka dalam borang tersebut dan diberikan pilihan untuk bersetuju dengan pemprosesan data peribadi yang mereka berikan dengan menandakan kotak semak. Secara lalai, kotak semak ini tidak ditandakan.

Kafe juga memastikan bahawa secara lalai hanya kuki yang benar-benar diperlukan diaktifkan. Kuki tambahan hanya akan diaktifkan apabila pelanggan secara jelas memberikan persetujuan bagi penggunaannya.

***Soalan 9***

***Apakah pandangan atau cadangan anda mengenai elemen utama DPbD bagi Prinsip Am?***

## [C.2] Prinsip Notis dan Pilihan

2.24 **Prinsip notis dan pilihan**[15] memerlukan pengawal data untuk bersikap jelas dan telus dengan subjek data mengenai cara mereka mengumpul, menggunakan dan berkongsi data peribadi.

2.25 Elemen utama PbD bagi prinsip ini termasuk:

(a) **Kejelasan**: Maklumat harus disampaikan dalam bahasa yang jelas, mudah difahami, ringkas dan tidak mengelirukan.

(b) **Semantik:** Komunikasi harus mempunyai makna yang tepat dan jelas bagi audiens yang disasarkan.

(c) **Kebolehcapaian:** Maklumat harus mudah diakses oleh subjek data tanpa halangan yang tidak perlu.

(d) **Kontekstual:** Maklumat harus diberikan pada masa yang sesuai dan dalam format yang paling relevan.

(e) **Keberkaitan**: Maklumat harus berkaitan secara langsung dengan subjek data dan tujuan pemprosesan data.

(f) **Reka bentuk universal**: Maklumat harus boleh diakses oleh semua subjek data termasuk melalui bahasa yang boleh dibaca mesin untuk meningkatkan kebolehbacaan dan pemprosesan automatik.

(g) **Boleh difahami**: Subjek data harus mempunyai pemahaman yang jelas tentang bagaimana data peribadi mereka akan diproses, terutamanya bagi kanak-kanak atau kumpulan rentan.

(h) **Pelbagai saluran**: Maklumat harus disampaikan melalui pelbagai platform dan media untuk memastikan ia sampai kepada subjek data secara efektif.

(i) **Berlapis**: Maklumat harus disusun dalam lapisan yang seimbang antara kelengkapan dan kefahaman dengan mengambil kira jangkaan munasabah subjek data.

2.26 Tidak boleh ada **corak reka bentuk yang mengelirukan**, iaitu antara muka dan perjalanan pengguna yang bertujuan mempengaruhi pengguna untuk membuat keputusan yang tidak disengajakan, tidak dikehendaki, dan/atau berkemungkinan membahayakan, selalunya ke arah pilihan yang bertentangan dengan kepentingan terbaik pengguna dan lebih memihak kepada kepentingan pengawal data.

[15] Akta 709, s. 7.

2.27 Contoh corak reka bentuk yang mengelirukan termasuk:

(a) **Beban berlebihan:** Pengguna berdepan dengan terlalu banyak permintaan, maklumat, pilihan atau langkah yang menyebabkan mereka secara tidak sengaja berkongsi lebih banyak data atau membenarkan pemprosesan data peribadi tanpa disedari.

(b) **Melangkau**: Reka bentuk antara muka atau aliran pengguna dibuat supaya mereka secara tidak sengaja mengabaikan atau tidak menyedari aspek perlindungan data, menyebabkan mereka memberikan persetujuan tanpa memahami sepenuhnya.

(c) **Mempengaruhi pilihan:** Menggunakan unsur emosi atau visual untuk mendorong pengguna membuat keputusan tertentu, seperti memaparkan mesej yang menekan mereka untuk memilih sesuatu yang lebih menguntungkan pengawal data.

(d) **Menyekat akses:** Pengguna sukar mendapatkan maklumat atau mengurus data mereka dengan menyembunyikan tetapan kawalan privasi dalam menu yang kompleks atau menambah langkah yang tidak perlu.

(e) **Tidak jelas dan mengelirukan:** Reka bentuk antara muka yang tidak konsisten atau rumit, menyukarkan pengguna untuk mencari tetapan perlindungan data dan memahami bagaimana data mereka diproses.

(f) **Dibiarkan dalam kegelapan:** Antaramuka direka dengan cara yang menyembunyikan maklumat atau alat kawalan perlindungan data, atau membuatkan pengguna tidak pasti tentang bagaimana data mereka diproses serta jenis kawalan yang mungkin mereka miliki ke atasnya berkenaan dengan pelaksanaan hak-hak mereka.

**Contoh praktikal pelaksanaan DPbD bagi Prinsip Notis dan Pilihan**

Kafe memastikan bahawa pelanggan diarahkan ke notis perlindungan data peribadi / privasi ketika mereka membuat pesanan atau mendaftar akaun keahlian. Notis perlindungan data peribadi / privasi ditulis dalam bahasa yang jelas dan ringkas supaya pelanggan dapat memahami dengan mudah bagaimana data peribadi mereka diproses. Maklumat disampaikan secara berlapis, di mana perkara yang paling penting diserlahkan, manakala maklumat terperinci disediakan dengan mudah untuk memberikan penjelasan lanjut mengenai pelbagai perkara dan konsep yang digunakan dalam notis tersebut. Notis perlindungan data peribadi / privasi tersedia dan kelihatan di semua halaman laman web, memastikan pelanggan sentiasa boleh mengakses maklumat tersebut dengan hanya satu klik.

***Soalan 10***

***(a) Apakah pandangan atau cadangan anda mengenai elemen utama DPbD bagi Prinsip Notis dan Pilihan?***

***(b) Bagaimana kita boleh memudahkan akses individu kurang upaya kepada notis perlindungan data peribadi / privasi?***

## [C.3] Prinsip Penzahiran

2.28 **Prinsip penzahiran**[16] mengkehendaki pengawal data untuk:

(a) mendapatkan persetujuan subjek data atau mempunyai asas undang-undang yang sah untuk sebarang penzahiran data peribadi;

(b) hanya mendedahkan data peribadi untuk tujuan yang dinyatakan semasa pengumpulan data peribadi; dan

(c) hanya mendedahkan data peribadi kepada kategori pihak ketiga yang dinyatakan dalam notis perlindungan data peribadi / privasi yang diberikan kepada subjek data.

2.29 Elemen utama DPbD bagi prinsip ini merangkumi:

(a) **Penentuan awal**: Asas undang-undang bagi penzahiran harus ditetapkan sebelum penzahiran dilakukan. Prinsip ini akan mempengaruhi reka bentuk penzahiran dan penetapan had penzahiran.

(b) **Pengelakan data**: Pengawal data harus mengelakkan penzahiran data peribadi sepenuhnya jika tujuan yang berkaitan dapat dicapai tanpa penzahiran. Data yang dipseudonimkan atau diagregatkan harus digunakan jika boleh.

(c) **Pembezaan**: Asas undang-undang dan tujuan yang digunakan untuk setiap aktiviti penzahiran harus dibezakan.

(d) **Keberkaitan:** Asas undang-undang yang betul mesti diterapkan dalam penzahiran dan mempunyai kaitan yang jelas dengan tujuan penzahiran. Data peribadi yang didedahkan harus relevan dengan penzahiran yang dilakukan dan pengawal data harus dapat menunjukkan keberkaitan ini.

(e) **Keperluan:** Tujuan penzahiran menentukan jenis data peribadi yang diperlukan untuk didedahkan. Setiap jenis data peribadi harus diperlukan bagi tujuan yang dinyatakan dan hanya boleh didedahkan jika tiada cara lain untuk memenuhi tujuan tersebut.

(f) **Semakan:** Semakan berkala harus dilakukan untuk mengesahkan sama ada penzahiran masih diperlukan bagi tujuan asal penzahiran data.

(g) **Penamatan:** Jika asas undang-undang dan tujuan penzahiran tidak lagi terpakai, data peribadi tidak boleh lagi didedahkan. Langkah-langkah kawalan dan perlindungan harus

[16] Akta 709, s. 8.

disediakan untuk memastikan pihak ketiga yang menerima data peribadi memusnahkan data tersebut dengan selamat.

(h) **Pelarasan:** Jika terdapat perubahan yang sah dalam asas undang-undang bagi penzahiran, penzahiran sebenar harus disesuaikan mengikut asas undang-undang yang baru.

(i) **Keselamatan:** Langkah teknikal seperti penceraian data dan penyulitan serta langkah pengurusan seperti dasar dan kewajipan kontrak harus dilaksanakan untuk memastikan data peribadi didedahkan dengan selamat.

**Contoh praktikal pelaksanaan DPbP bagi Prinsip Penzahiran**

Kafe tersebut memetakan aliran data untuk mengenal pasti jenis data peribadi yang akan didedahkan kepada pihak ketiga serta memastikan bahawa terdapat asas undang-undang bagi penzahiran tersebut dan pelanggan telah dimaklumkan mengenainya. Memandangkan data peribadi akan didedahkan kepada penyedia sistem pesanan dalam talian bagi tujuan penyelenggaraan sandar dan log, kafe ini memastikan bahawa perjanjian dengan penyedia tersebut secara jelas menetapkan peranan dan tanggungjawab setiap pihak dalam mengendalikan data peribadi serta membenarkan kafe menjalankan audit bagi mengesahkan pematuhan terhadap tanggungjawab tersebut.

***Soalan 11***

***Apakah pandangan atau cadangan anda mengenai elemen utama DPbD bagi Prinsip Penzahiran?***

## [C.4] Prinsip Keselamatan

2.30 **Prinsip keselamatan**[17] mengkehendaki pengawal data dan pemproses data untuk mengambil langkah-langkah praktikal bagi melindungi data peribadi daripada sebarang kehilangan, salah guna, ubah suaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan.

2.31 Elemen utama DPbD bagi prinsip ini merangkumi:

(a) **Sistem pengurusan keselamatan maklumat (ISMS):** Mempunyai cara operasi mengurus dasar dan prosedur bagi keselamatan maklumat.

(b) **Analisis risiko:** Menilai risiko terhadap keselamatan data peribadi dengan mempertimbangkan kesannya terhadap hak individu serta mengambil langkah untuk mengurangkan ancaman yang telah dikenal pasti. Dalam membuat penilaian risiko;

[17] Akta 709, s. 9.

membangunkan dan mengekalkan “pemodelan ancaman” yang menyeluruh, sistematik dan realistik serta analisis permukaan serangan *(attack surface analysis)* berkenaan perisian yang direka bentuk untuk mengurangkan serangan vektor dan peluang untuk pengeksploitasian titik kelemahan dan pendedahan pada bahaya .

(c) **Mereka bentuk berdasarkan keselamatan:** Mempertimbangkan keperluan keselamatan dalam reka bentuk dan pembangunan sistem seawal mungkin serta menjalankan ujian dan pengintegrasian berterusan.

(d) **Penyelenggaraan:** Sering menguji dan memeriksa perisian, perkakasan, sistem dan perkhidmatan bagi mengesan sama ada sistem yang menyokong pemprosesan terdedah pada bahaya.

(e) **Pengurusan kawalan akses:** Hanya kakitangan yang diberi kuasa dan memerlukan akses kepada data peribadi untuk tugas pemprosesan sahaja yang sepatutnya diberikan akses dan keistimewaan akses sewajarnya dibezakan.

(f) **Pengehadan akses:** Pemprosesan data sepatutnya dihadkan kepada jumlah individu yang amat sedikit yang memerlukan akses untuk melaksanakan tugas-tugas mereka.

(g) **Pengehadan akses (kandungan):** Bagi setiap operasi pemprosesan, hadkan akses hanya kepada ciri-ciri dalam set data yang diperlukan untuk menjalankan operasi tersebut. Selain itu, hadkan akses hanya kepada data subjek yang berada dalam skop tanggungjawab kakitangan yang berkenaan.

(h) **Pengasingan akses**: Pastikan pemprosesan data tidak membenarkan mana-mana individu mempunyai akses penuh kepada semua data yang dikumpulkan mengenai seseorang subjek data, lebih-lebih lagi semua data peribadi bagi kategori subjek data tertentu.

(i) **Pemindahan selamat:** Pemindahan data mesti dilindungi daripada akses dan perubahan tanpa kebenaran atau tidak sengaja.

(j) **Penyimpanan selamat:** Penyimpanan data mesti dilindungi daripada akses dan perubahan yang tidak dibenarkan. Sewajarnya ada prosedur untuk menilai risiko penyimpanan secara terpusat *(centralized)* atau ternyahpusat *(decentralized)* serta kategori data peribadi yang terlibat. Sesetengah data mungkin memerlukan langkah keselamatan tambahan atau pengasingan daripada data lain.

(k) **Pseudonimisasi**: Data peribadi harus dipseudonimkan sejurus selepas ia tidak lagi diperlukan sebagai data peribadi yang boleh terus dikenal pasti. Ini dilakukan sebagai langkah keselamatan untuk mengurangkan risiko kebocoran data, contohnya menggunakan penceraian data atau penyulitan. Kunci pengecaman harus disimpan secara berasingan.

(l) **Sandar/log:** Simpan *sandar (back-up)* dan log setakat yang diperlukan bagi keselamatan maklumat dan gunakan jejak audit serta pemantauan kejadian sebagai kawalan keselamatan rutin. Sandar/log perlu dilindungi daripada akses dan perubahan yang tidak dibenarkan serta

tidak sengaja dan dikaji semula secara berkala. Apa-apa insiden sewajarnya ditangani dengan segera.

(m) **Pemulihan bencana / kesinambungan perniagaan:** Kemukakan sistem maklumat pemulihan bencana dan kesinambungan perniagaan bagi memulihkan data peribadi yang sedia ada selepas insiden besar.

(n) **Perlindungan mengikut risiko:** Semua kategori data peribadi harus dilindungi menggunakan langkah keselamatan yang bersesuaian dengan tahap risiko pelanggaran keselamatan. Jika boleh, data yang mempunyai risiko khas harus diasingkan daripada data peribadi lain.

(o) **Pengurusan respons insiden keselamatan:** Menyediakan rutin, prosedur dan sumber yang mencukupi untuk mengesan, mengawal, menangani, melaporkan serta mempelajari daripada pelanggaran data.

(p) **Pengurusan insiden:** Menyediakan proses untuk menangani pelanggaran dan insiden untuk menjadikan sistem pemprosesan lebih berkesan. Ini termasuk prosedur pemberitahuan kepada pihak pengawal selia dan subjek data.

**Contoh praktikal pelaksanaan DPbP bagi Prinsip Keselamatan**[18]

Kafe tersebut memastikan bahawa privasi diterapkan dalam sistem pesanan dalam talian. Data peribadi pelanggan disimpan dan diproses dalam sistem pangkalan data yang berasingan yang menggunakan kunci penyulitan dengan tahap kepanjangan berbeza bergantung pada jenis data. Selain itu, sebelum sistem dilancarkan, penilaian risiko dilakukan terhadap infrastruktur IT untuk memastikan ia berfungsi seperti yang dijangkakan sebelum digunakan secara rasmi. Penilaian ini juga dijalankan secara berkala selepas sistem beroperasi.

***Soalan 12***

***Apakah pandangan atau cadangan anda mengenai elemen utama DPbD bagi Prinsip Keselamatan?***

## [C.5] Prinsip Penyimpanan

2.32 **Prinsip penyimpanan**[19] mengkehendaki pengawal data untuk tidak menyimpan data peribadi yang diproses lebih lama daripada yang diperlukan untuk memenuhi tujuan tersebut.

2.33 Elemen utama DPbD bagi prinsip ini merangkumi:

[18] Berdasarkan kepada https://www.dpoconsultancy.com/liveblog/a-practical-example-of-how-to-apply-privacy-by-design.
[19] Akta 709, s. 10.

(a) **Pengurangan data:** Semasa data peribadi diproses selanjutnya, pengawal data wajar dari semasa ke semasa mempertimbangkan sama ada data yang diproses masih mencukupi, relevan dan diperlukan atau sama ada data tersebut perlu dipadamkan. Jika tujuan pemprosesan tidak memerlukan set data yang muktamad untuk merujuk kepada individu yang dikenal pasti atau boleh dikenal pasti (seperti dalam statistik) tetapi pemprosesan awal memerlukannya (contohnya sebelum data diagregatkan) maka pengawal data perlu memadamkan data peribadi sebaik sahaja pengecaman tidak lagi diperlukan.

(b) **Pemadaman dan anonimisasi:** Jika data peribadi tidak atau tidak lagi diperlukan bagi tujuan pemprosesan, data tersebut harus dianonimkan atau dipadamkan. Prosedur dalaman yang jelas dan kefungsian untuk proses pemadaman dan/atau anonimisasi wajar disediakan.

(c) **Keberkesanan anonimisasi/pemadaman:** Pengawal data harus memastikan bahawa data yang telah dianonimkan tidak boleh dikenal pasti semula dan data yang telah dipadamkan tidak boleh dikembalikan. Pengawal data wajar menguji untuk menentukan sama ada ia boleh dilakukan.

(d) **Automasi**: Pemadaman data peribadi tertentu harus dilakukan secara automatik.

(e) **Kriteria penyimpanan**: Pengawal data harus menentukan jenis data dan tempoh penyimpanan yang diperlukan bagi memenuhi tujuannya.

(f) **Justifikasi:** Pengawal data wajar memberikan justifikasi mengapa tempoh penyimpanan diperlukan untuk tujuan pemprosesan dan data peribadi yang berkaitan. Pengawal data juga seharusnya dapat menerangkan rasional di sebalik tempoh penyimpanan tersebut serta asas undang-undangnya.

(g) **Penguatkuasaan dasar penyimpanan**: Pengawal data harus menguatkuasakan polisi penyimpanan dalaman dan menjalankan ujian terhadap pematuhan polisi tersebut.

(h) **Sandar/log**: Pengawal data harus menentukan jenis data peribadi dan tempoh penyimpanan yang diperlukan bagi sandar dan log.

(i) **Aliran data:** Pengawal data harus peka berkenaan aliran data peribadi serta lokasi penyimpanan mana-mana salinan data dan berusaha untuk mengehadkan penyimpanan "sementara" yang tidak perlu. Aliran data harus diurus dengan cekap bagi mengelakkan penciptaan salinan data yang berlebihan.

**Contoh praktikal pelaksanaan DPbP bagi Prinsip Penyimpanan**

Pangkalan data yang menyimpan data peribadi pelanggan direka bentuk supaya tempoh penyimpanan bagi setiap data peribadi dijana secara automatik semasa ia ditambah ke dalam pangkalan data dan data peribadi yang mencapai tempoh penyimpanan akan dipadam secara automatik.

***Soalan 13***

***Apakah pandangan atau cadangan anda mengenai elemen utama DPbD bagi Prinsip Penyimpanan?***

## [C.6] Prinsip Integriti Data

2.34 **Prinsip integriti data**[20] memerlukan pengawal data untuk mengambil langkah yang munasabah bagi memastikan data peribadi adalah tepat, lengkap, tidak mengelirukan dan dikemas kini dengan mengambil kira tujuan data peribadi dikumpulkan dan diproses selanjutnya.

2.35 Elemen utama DPbD bagi prinsip ini merangkumi:

(a) **Sumber data:** Sumber data peribadi mestilah boleh dipercayai dari segi ketepatan data.

(b) **Tahap ketepatan:** Setiap elemen data peribadi haruslah setepat yang diperlukan untuk tujuan yang ditetapkan.

(c) **Ketepatan boleh diukur:** Kurangkan jumlah keputusan positif palsu (contohnya, aplikasi penjejakan kontak memberi amaran kepada individu yang salah bahawa mereka telah terdedah kepada penyakit berjangkit dan berisiko tinggi) / keputusan negatif palsu (contohnya, aplikasi penjejakan kontak gagal memberi amaran kepada individu yang sebenarnya berisiko tinggi) sebagai contoh, keputusan automatik dan kecerdasan buatan yang berat sebelah.

(d) **Pengesahan:** Bergantung pada sifat data dan seberapa kerap ia mungkin berubah, pengawal data wajar mengesahkan ketepatan data peribadi dengan subjek data sebelum dan pada pelbagai peringkat pemprosesan (contohnya, bagi keperluan umur).

(e) **Pembetulan**: Pengawal data wajar memudahkan pembetulan data yang tidak tepat dengan segera apabila diminta oleh subjek data.

(f) **Pencegahan penyebaran ralat:** Pengawal data harus mengurangkan kesan kesilapan yang terkumpul dalam rantaian pemprosesan.

(g) **Akses:** Subjek data harus diberikan maklumat serta akses yang berkesan kepada data peribadi mereka mengikut prinsip akses bagi mengawal ketepatan dan membuat pembetulan jika perlu.

(h) **Ketepatan berterusan:** Data peribadi harus kekal tepat pada semua peringkat pemprosesan dan ujian ketepatan harus dijalankan pada setiap langkah kritikal.

(i) **Dikemas kini:** Data peribadi harus dikemas kini jika perlu untuk tujuannya.

[20] Akta 709, s. 11.

(j) **Reka bentuk data:** Penggunaan reka bentuk teknologi dan pengurusan untuk mengurangkan ketidaktepatan. Sebagai contoh, mengemukakan pilihan pratetap ringkas dan jelas berbanding medan teks bebas.

**Contoh praktikal pelaksanaan DPbP bagi Prinsip Integriti Data**

Lihat contoh yang disediakan di bawah **C.7 (Prinsip Akses)**.

***Soalan 14***

***Apakah pandangan atau cadangan anda mengenai elemen utama DPbD bagi Prinsip Integriti Data?***

## [C.7] Prinsip Akses

2.36 **Prinsip akses**[21] mengkehendaki pengawal data untuk membenarkan subjek data mengakses data peribadi mereka dan membetulkan data yang tidak tepat, tidak lengkap, mengelirukan atau tidak dikemas kini[22] serta menarik balik persetujuan terhadap pemprosesan data peribadi mereka.[23] Subjek data sepatutnya mengetahui dengan mudah kepada siapa mereka perlu mengemukakan permintaan apabila ingin melaksanakan hak mereka. Maklumat hubungan harus mudah diakses dan diletakkan di lokasi yang lojik seperti dalam akaun pengguna, dalam maklumat kontekstual, notis perlindungan data peribadi / privasi, bahagian FAQ dan sebagainya.

2.37 Elemen utama DPbD bagi prinsip ini merangkumi:

(a) **Kejelasan:** Maklumat tentang bagaimana untuk melaksanakan hak subjek data harus disampaikan dalam bahasa yang jelas, mudah difahami, ringkas dan tidak mengelirukan.

(b) **Kebolehcapaian:** Mekanisme untuk melaksanakan hak subjek data harus mudah diakses oleh mereka.

(c) **Kontekstual:** Mekanisme untuk melaksanakan hak subjek data harus disediakan pada masa yang relevan dan dalam format yang sesuai.

(d) **Reka bentuk universal:** Mekanisme untuk melaksanakan hak subjek data harus boleh diakses oleh semua subjek data termasuk penggunaan bahasa yang boleh dibaca mesin bagi memudahkan dan mengautomasikan kebolehbacaan serta kejelasan.

(e) **Boleh difahami:** Subjek data harus mempunyai pemahaman yang jelas mengenai sejauh mana mereka boleh melaksanakan hak mereka dan apa yang boleh mereka jangkakan.

[21] Akta 709, s. 6.
[22] Akta 709, s. 12.
[23] Akta 709, s. 38.

(f) **Pelbagai saluran:** Mekanisme untuk melaksanakan hak subjek data harus disediakan melalui pelbagai saluran dan media bukan hanya dalam bentuk teks bagi meningkatkan kemungkinan maklumat sampai kepada subjek data secara berkesan.

**Contoh praktikal pelaksanaan DPbD bagi Prinsip Akses**

Kafe tersebut memastikan bahawa para pelanggan dapat menggunakan hak mereka terhadap data peribadi mereka dengan mudah. Dalam profil akaun mereka, terdapat pilihan pantas untuk pelanggan memuat turun data peribadi mereka dalam format yang mudah diakses, mengedit data peribadi mereka dan memadam akaun mereka. Pelanggan dimaklumkan serta-merta mengenai penerimaan permintaan mereka, diberikan maklumat tentang cara menjejak kemajuan permintaan tersebut serta cara menghubungi pihak perniagaan sekiranya mereka memerlukan bantuan lanjut.

***Soalan 15***

***Apakah pandangan atau cadangan anda mengenai elemen utama DPbD bagi Prinsip Akses?***

## [D] Melindungi privasi kanak-kanak

2.38 **Latar belakang:** Kanak-kanak layak mendapat perlindungan khusus berkaitan dengan data peribadi mereka kerana mereka sering kurang menyedari (disebabkan oleh umur, kematangan dan kapasiti perkembangan mereka) mengenai risiko, akibat, langkah-langkah keselamatan serta hak-hak mereka berkaitan dengan pemprosesan data peribadi mereka.

2.39 Walaupun hak privasi kanak-kanak lazimnya dianggap sebagai perkara yang ditentukan oleh orang dewasa, keperluan privasi kanak-kanak sebenarnya boleh berbeza dan malah bercanggah dengan keperluan orang dewasa. Tafsiran orang dewasa terhadap keperluan privasi kanak-kanak boleh mengehadkan hak kanak-kanak terhadap privasi dan autonomi mereka. Contohnya, kebergantungan orang dewasa kepada pengawasan bagi tujuan perlindungan serta trend "*sharenting*" yang semakin meluas—di mana ibu bapa menyiarkan maklumat tentang anak-anak mereka dalam talian, yang secara tidak langsung membentuk identiti dalam talian kanak-kanak tersebut sebelum mereka mampu memberi persetujuan. Tambahan pula, kanak-kanak tanpa persekitaran rumah yang stabil, seperti kanak-kanak jalanan, kanak-kanak tanpa pengiring, kanak-kanak dalam jagaan "di luar rumah," atau kanak-kanak lain yang berada dalam situasi rentan mungkin tidak mendapat sokongan dan bimbingan mencukupi daripada orang dewasa untuk melindungi privasi mereka.

2.40 Maka, pengawal data mempunyai tanggungjawab kritikal untuk memastikan bahawa produk dan perkhidmatan yang mereka tawarkan berteraskan konsep mereka bentuk berdasarkan perlindungan data peribadi kanak-kanak supaya kanak-kanak dapat meraih manfaat daripada penyertaan mereka baik secara dalam dan luar talian dengan selamat.

2.41 **Cadangan:** Dicadangkan agar Garis Panduan DPbD memasukkan panduan khusus serta keperluan preskriptif berhubung pelaksanaan DPbD bagi operasi pemprosesan data yang melibatkan data peribadi kanak-kanak.

***Soalan 15***

***Apakah pandangan / cadangan anda mengenai pemprosesan data peribadi kanak-kanak dalam Garis Panduan DPbD?***

**[D.1] Skop pengaplikasian**

2.42 **Cadangan:** Dicadangkan bahawa penyedia produk atau perkhidmatan yang ditujukan kepada, bertujuan untuk atau berkemungkinan diakses oleh kanak-kanak akan dikehendaki mematuhi seksyen ini bagi tujuan perlindungan privasi kanak-kanak selaras dengan DPbD.

2.43 Dalam konteks luar talian, ia merangkumi penyedia pendidikan, kelab sukan dan sosial serta komuniti dan penyedia kesihatan serta sokongan sosial. Dalam konteks digital, ia merangkumi laman web, aplikasi dan perkhidmatan Internet Pelbagai Benda (IoT) lain yang menyediakan media sosial, perkongsian media, permainan, hiburan, pendidikan, advokasi atau perkhidmatan sokongan sosial. Skop ini juga mesti meliputi perkhidmatan yang digunakan oleh sejumlah besar kanak-kanak walaupun produk atau perkhidmatan tersebut bukan pada asalnya bertujuan untuk kanak-kanak atau direka bentuk dengan mengambil kira kegunaan oleh kanak-kanak.

***Soalan 16***

***(a) Apakah pandangan / cadangan anda mengenai skop pengaplikasian?***

***(b) Adakah pengecualian harus diberikan?***

**[D.2] Kepentingan terbaik bagi kanak-kanak**

2.44 **Cadangan:** Dicadangkan bahawa pengawal data mempunyai kewajipan untuk mengambil kira kepentingan terbaik bagi kanak-kanak dalam pemprosesan data peribadi mereka apabila produk atau perkhidmatan yang ditawarkan disasarkan kepada, bertujuan untuk atau berkemungkinan diakses oleh kanak-kanak.

2.45 Konsep kepentingan terbaik bagi kanak-kanak berasal daripada Perkara 3 Konvensyen Bangsa-Bangsa Bersatu mengenai Hak Kanak-Kanak yang menyatakan:

*"Dalam semua tindakan yang melibatkan kanak-kanak, sama ada yang dilakukan oleh institusi kebajikan sosial awam atau swasta, mahkamah, pihak berkuasa pentadbiran atau badan perundangan, kepentingan terbaik bagi kanak-kanak hendaklah menjadi pertimbangan utama."*

2.46 Pengawal data wajar mempertimbangkan bagaimana dalam penggunaan data peribadi kanak-kanak, mereka dapat:

(a) memastikan kanak-kanak selamat daripada risiko eksploitasi, termasuk eksploitasi komersial, eksploitasi seksual dan penderaan seksual;

(b) melindungi serta menyokong kesihatan dan kesejahteraan kanak-kanak;

(c) melindungi serta menyokong perkembangan fizikal, psikologi dan emosi kanak-kanak;

(d) melindungi serta menyokong keperluan kanak-kanak untuk membentuk pandangan dan identiti mereka sendiri;

(e) melindungi serta menyokong hak kanak-kanak terhadap kebebasan berpersatuan dan aktiviti permainan;

(f) menyokong keperluan kanak-kanak kurang upaya;

(g) mengiktiraf peranan ibu bapa dalam melindungi dan mempromosikan kepentingan terbaik kanak-kanak serta menyokong mereka dalam tugas ini; dan

(h) mengiktiraf keupayaan kanak-kanak yang semakin berkembang untuk membentuk pandangan sendiri serta memberikan pertimbangan sewajarnya terhadap pandangan mereka.

2.47 Mengambil kira kepentingan terbaik bagi kanak-kanak tidak bermaksud pengawal data tidak boleh mengejar kepentingan komersial atau kepentingan mereka yang lain. Kepentingan komersial pengawal data tidak semestinya bercanggah dengan kepentingan terbaik kanak-kanak tetapi jika terdapat sebarang konflik, kepentingan terbaik kanak-kanak mesti menjadi pertimbangan utama.

***Soalan 17***

***(a) Apakah pandangan anda mengenai keperluan bagi pengawal data untuk mengambil kira kepentingan terbaik bagi kanak-kanak dalam pemprosesan data peribadi mereka apabila produk atau perkhidmatan yang ditawarkan disasarkan kepada, bertujuan untuk atau berkemungkinan diakses oleh kanak-kanak?***

***(b) Apakah pandangan anda mengenai elemen yang harus diambil kira dalam menilai kepentingan terbaik bagi kanak-kanak?***

## [D.3] Pengesahan umur

2.48 **Cadangan:** Selari dengan GDPR,[24] keperluan yang jelas harus diperkenalkan ke atas pengawal data untuk mengambil usaha yang munasabah dalam mengesahkan bahawa mereka telah menerima persetujuan untuk memproses data peribadi kanak-kanak. Dalam keadaan tertentu, ini merangkumi keperluan untuk mewujudkan mekanisme pengesahan umur.

2.49 Secara amnya, tidak terdapat penyelesaian yang seragam bagi isu pengesahan umur. Mekanisme pengesahan umur yang sesuai mungkin berbeza mengikut konteks bergantung kepada faktor seperti jenis perkhidmatan yang disediakan dan tahap sensitiviti data peribadi yang diproses. Walau apa pun, langkah-langkah pengesahan umur harus seimbang dan berdasarkan pendekatan berasaskan risiko. Ini bermaksud bahawa semakin tinggi risiko yang ditimbulkan oleh pemprosesan data, semakin ketat proses pengesahan yang diperlukan. Sebagai contoh, pengisytiharan kendiri mungkin mencukupi untuk pemprosesan data berisiko rendah atau apabila digabungkan dengan teknik lain. Namun, bagi perkhidmatan dalam talian yang melibatkan risiko tinggi akibat pemprosesan data, kaedah pengesahan umur yang lebih ketat mungkin diperlukan.

2.50 Berikut ialah senarai mekanisme pengesahan umur yang lazimnya digunakan:[25]

(a) **Pengisytiharan kendiri:** Kaedah yang paling biasa digunakan ini telah terbukti paling mudah dielakkan oleh kanak-kanak. Contohnya termasuk pengisytiharan tarikh lahir sendiri.

(b) **Kad kredit:** Pengguna dikehendaki mengesahkan kesahihan kad mereka, contohnya dengan membuat pembayaran RM0.01 kepada bank atau syarikat kad kredit. Kaedah ini biasanya digunakan oleh laman e-dagang dan aplikasi yang menjual produk dewasa seperti alkohol atau kandungan dewasa. Selain risiko pemancingan data *(phishing)*, kaedah ini tidak dapat memastikan bahawa pengguna kad adalah pemilik sahnya dan umur minimum pemilikan kad kredit juga berbeza mengikut negara.

(c) **Biometrik:** Kaedah ini menggunakan kecerdasan buatan (AI) untuk menggerakkan teknologi biometrik termasuk pengecaman wajah. Contohnya, aplikasi boleh menganalisis ciri wajah melalui swafoto bagi memastikan individu yang ingin mendapatkan akses berumur lebih 18 tahun. Walau bagaimanapun, kaedah ini boleh terdedah kepada ralat dan kanak-kanak boleh menggunakan wajah individu yang lebih tua untuk mendapatkan akses. Selain itu, kaedah ini menimbulkan isu privasi kerana melibatkan data peribadi sensitif dan boleh membawa kepada pemprosesan data secara berlebihan serta pemprofilan.

(d) **Sistem pengesahan umur secara inferens**: Kaedah ini menggunakan sistem yang membuat anggaran umur berdasarkan sejarah pelayaran internet individu, analisis "kematangan" melalui soal selidik, kandungan dalam talian yang dijana pengguna atau corak pembelian mereka.

(e) **Pengesahan luar talian**: Kaedah ini menggunakan kad gores atau pemeriksaan umur secara fizikal melalui dokumen pengenalan. Sebagai contoh, perkhidmatan dalam talian boleh meminta individu dewasa mendapatkan "kad gores" yang memberikan mereka pengecam log

[24] GDPR, Art. 8(2).
[25] Rujukan: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.

masuk dan kata laluan untuk mengakses kandungan yang terhad mengikut umur. Kad ini boleh dijual di kedai tertentu seperti pasar raya atau kedai tembakau di mana kakitangan sudah biasa menjalankan pemeriksaan umur bagi jualan alkohol, rokok dan perjudian.

(f) **Pengesahan persetujuan ibu bapa:** Kaedah ini boleh melibatkan semakan dokumen pengenalan diri (ID) tradisional.

(g) **Jaminan pihak ketiga:** Ini melibatkan pengguna selain ibu bapa untuk menjamin dalam talian sebagai pengesahan bahawa kanak-kanak yang ingin mengakses perkhidmatan dalam talian adalah dalam lingkungan umur yang dibenarkan.

(h) **ID digital:** Kaedah ini bergantung pada kaedah yang disediakan oleh Kerajaan untuk mengesahkan identiti dan umur individu sebelum membenarkan akses ke perkhidmatan digital. Sebagai contoh, China, Kanada dan Australia telah memperkenalkan ID digital untuk warganegara mereka. Beberapa negara di EU juga telah mengguna pakai penyelesaian ini dan terdapat cadangan untuk mewujudkan dompet identiti digital Eropah.

2.51 Perlu ditekankan bahawa pematuhan terhadap keperluan ini sama sekali tidak boleh digunakan sebagai alasan untuk menghalang kanak-kanak daripada mendapatkan perkhidmatan dalam talian atau untuk menyediakan pendekatan 2 peringkat di mana pengguna kanak-kanak diberikan perkhidmatan asas yang kurang lengkap manakala pengguna dewasa diberikan perkhidmatan yang lebih baik, semata-mata atas alasan pematuhan perlindungan data. Pendekatan seperti ini boleh dilihat oleh kanak-kanak sebagai sekatan terhadap akses mereka kepada perkhidmatan penuh atau ciri lain dalam perkhidmatan yang mereka ingin gunakan. Ia juga berisiko menyebabkan kanak-kanak mencari jalan lain seperti menipu umur mereka untuk mendapatkan akses kepada perkhidmatan yang mereka anggap lebih lengkap dan sesuai untuk orang dewasa. Keadaan ini boleh memberi kesan negatif kepada organisasi kerana ia mungkin mengakibatkan kanak-kanak memintas langkah pengesahan umur dan menggunakan perkhidmatan yang tidak mematuhi standard perlindungan data tertinggi yang diperlukan untuk kanak-kanak.

2.52 **Pengesahan persetujuan ibu bapa:** GDPR pada masa ini menetapkan bahawa pengguna data mesti mendapatkan persetujuan daripada ibu bapa, penjaga atau individu yang mempunyai tanggungjawab penjagaan terhadap subjek data jika subjek data berumur di bawah 18 tahun. Selaras dengan GDPR, keperluan yang jelas harus diperkenalkan bagi pengawal data untuk mengambil langkah yang munasabah dalam mengesahkan bahawa persetujuan telah diberikan oleh ibu bapa, penjaga atau individu yang bertanggungjawab terhadap kanak-kanak dengan mengambil kira teknologi yang tersedia. Pendekatan berdasarkan risiko dan kadar yang seimbang harus diterapkan, di mana tahap keketatan dan ketepatan pengesahan meningkat sekiranya pemprosesan data peribadi yang dilakukan oleh organisasi menimbulkan risiko yang lebih tinggi kepada kanak-kanak. Sebagai contoh, bagi pemprosesan berisiko rendah, pengesahan mungkin hanya memerlukan penghantaran e-mel pengesahan kepada ibu bapa yang mesti mereka sahkan. Namun, bagi pemprosesan yang melibatkan risiko lebih tinggi, kaedah pengesahan yang lebih ketat seperti permintaan bukti ID mungkin diperlukan.

2.53 **Had umur minimum pengguna:** Amalan biasa dalam kalangan penyedia perkhidmatan dalam talian ialah menetapkan had umur minimum pengguna. Walau bagaimanapun, penetapan had umur minimum tidak mengecualikan keperluan penyedia perkhidmatan untuk mematuhi tanggungjawab

mereka terhadap pengguna kanak-kanak di bawah umur tersebut sekiranya mereka masih terdapat kemungkinan bahawa mereka akan menggunakan perkhidmatan tersebut. Jika penyedia perkhidmatan menyatakan bahawa perkhidmatan mereka tidak boleh digunakan oleh kanak-kanak di bawah usia tertentu, mereka harus memastikan bahawa mekanisme pengesahan umur yang digunakan adalah berkesan dalam menghalang akses kanak-kanak di bawah umur tersebut. Jika sesebuah organisasi mendapati bahawa mereka tidak dapat sepenuhnya menghalang akses kanak-kanak di bawah had umur yang ditetapkan, mereka harus memastikan bahawa langkah perlindungan data yang sesuai diterapkan bagi melindungi pengguna kanak-kanak, sama ada mereka berada di bawah atau melebihi had umur rasmi yang ditetapkan oleh organisasi tersebut.

***Soalan 18***

***(a) Apakah pandangan anda mengenai keperluan bagi pengawal data untuk mengambil langkah yang munasabah dalam mengesahkan bahawa mereka telah menerima persetujuan untuk memproses data peribadi kanak-kanak?***

***(b) Adakah anda menjangkakan sebarang kesukaran praktikal dalam melaksanakan keperluan ini?***

## [D.4] Pelaksanaan DPbD dalam pemprosesan data peribadi kanak-kanak

2.54 Organisasi harus memastikan bahawa tetapan privasi yang paling ketat digunakan untuk perkhidmatan yang disasarkan kepada, bertujuan untuk atau berkemungkinan diakses oleh kanak-kanak. Prinsip dan langkah DPbD yang diterangkan dalam seksyen di atas mengenai pelaksanaan DPbD dalam setiap **Prinsip PDP** harus diambil kira.

2.55 Pertimbangan khusus harus diberikan untuk menyediakan **notis dan pilihan** yang sesuai mengikut umur kanak-kanak.

2.56 Elemen utama DPbD merangkumi:

(a) **Bahasa:** Pengawal data mesti menggunakan bahasa yang jelas, ringkas dan mesra kanak-kanak untuk menerangkan dengan tepat kepada mereka apa yang dilakukan terhadap data peribadi mereka. Kanak-kanak sering tidak menyedari bahawa data peribadi merangkumi perkara seperti foto atau video mereka atau bahawa data mereka dikumpulkan untuk tujuan tertentu seperti menyediakan pengalaman dalam aplikasi yang disesuaikan dan pengiklanan atau bahawa data mereka akan disimpan untuk tempoh tertentu.

(b) **Kebolehcapaian:** Maklumat harus disediakan di tempat yang jelas dan mudah dicari, contohnya bukan dalam tulisan kecil di bahagian bawah laman web atau skrin aplikasi. Maklumat tidak boleh dipaparkan dengan cara yang menggalakkan pengguna untuk bersetuju tanpa berfikir terlebih dahulu seperti melalui tetingkap timbul *(pop-up)* yang menjadikan pilihan untuk bersetuju lebih ketara atau kurang mengganggu pengalaman pengguna berbanding pilihan untuk mengetahui lebih lanjut atau menolak persetujuan. Kanak-kanak tidak

seharusnya perlu mencari maklumat ini secara aktif. Pengawal data juga harus mempertimbangkan jenis peranti yang digunakan untuk mengakses perkhidmatan (contohnya, telefon pintar, komputer, peranti bersambung atau mainan), sama ada kaedah komunikasi bukan teks seperti kartun dan video lebih sesuai berbanding kaedah teks sahaja atau sama ada pemberitahuan elektronik seperti notis berlapis, notis layang atas (hover-over), atau notis tetingkap timbul adalah lebih sesuai.

(c) **Konteks**: Maklumat tidak boleh hanya diberikan semasa pendaftaran perkhidmatan atau ketika data peribadi mula dikumpulkan. Organisasi harus mempertimbangkan penggunaan kaedah seperti pemberitahuan tepat pada masanya *(just-in-time)* untuk memaklumkan kanak-kanak dan remaja mengenai implikasi perkongsian data peribadi mereka pada masa tertentu, contohnya sebelum mereka menyiarkan atau berkongsi sesuatu dalam talian atau sebelum mereka menukar tetapan privasi lalai.

(d) **Papan pemuka ibu bapa:** Jika sesuai, ibu bapa harus diberikan gambaran keseluruhan aktiviti (termasuk sejarah aktiviti) serta tetapan yang tersedia untuk anak mereka. Akaun kanak-kanak harus menyediakan maklumat mengenai fungsi papan pemuka ini.

***(e)*** **Penggunaan hak subjek data**: Pengawal data harus menyediakan aliran pengguna yang khusus, jelas dan mesra kanak-kanak bagi membolehkan mereka dan/atau ibu bapa atau penjaga mereka melaksanakan hak perlindungan data dengan mudah.

Bagi organisasi yang menggunakan alat automatik untuk mengurus permintaan subjek data, pertimbangan harus dibuat sejak peringkat reka bentuk aliran pengguna bagi mengenal pasti keadaan di mana pengecualian mungkin diperlukan, yang memerlukan penilaian individu (iaitu tidak sepenuhnya automatik dan melibatkan penglibatan manusia dalam proses penilaian). Penilaian ini harus mengambil kira konteks pemprosesan data peribadi yang terlibat dan menilai sama ada penggunaan sistem automatik melalui alat layan diri adalah sesuai untuk subjek data kanak-kanak. Secara umumnya, jika sesebuah organisasi menganggap bahawa perkhidmatan mereka sesuai untuk pengguna kanak-kanak di atas usia tertentu yang boleh berinteraksi secara autonomi dengan perkhidmatan tersebut maka kanak-kanak tersebut juga sepatutnya dapat melaksanakan hak perlindungan data mereka sendiri terhadap perkhidmatan atau organisasi tersebut.

***Soalan 19***

***Apakah pandangan / cadangan anda mengenai elemen utama DPbD bagi pemprosesan data peribadi kanak-kanak?***

## [D.5] Larangan pemprofilan atau pembuatan keputusan secara automatik berkaitan kanak-kanak

2.57 **Cadangan:** Dicadangkan bahawa pengawal data tidak boleh membuat pemprofilan terhadap kanak-kanak, terlibat dalam pembuatan keputusan secara automatik berkaitan kanak-kanak atau menggunakan data peribadi mereka untuk tujuan pengiklanan/pemasaran kecuali jika mereka dapat

dengan jelas menunjukkan bagaimana dan mengapa tindakan tersebut adalah demi kepentingan terbaik kanak-kanak.

***Soalan 20***

***(a) Apakah pandangan anda mengenai larangan pemprofilan atau pembuatan keputusan secara automatik berkaitan kanak-kanak?***

***(b) Apakah situasi di mana pengecualian harus diberikan?***