KEMENTERIAN DIGITAL

GARIS PANDUAN
PERLINDUNGAN DATA PERIBADI

MEREKA BENTUK BERDASARKAN PERLINDUNGAN DATA (DPbD)

Versi 1.0
Tarikh Terbitan: 30 April 2026

JABATAN PERLINDUNGAN DATA PERIBADI

Alamat:

JABATAN PERLINDUNGAN DATA PERIBADI
Aras 8, Galeria PjH, Jalan P4W, Persiaran Perdana
Presint 4, Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya, Malaysia

ISI KANDUNGAN

BAHAGIAN A: PENGENALAN

1. Latar belakang

1.1 Garis Panduan Mereka Bentuk Berdasarkan Perlindungan Data ("**Garis Panduan**") menggariskan panduan mengenai pengaplikasian pendekatan Mereka Bentuk Berdasarkan Perlindungan Data ("**DPbD**") kepada pengawal data dan pemproses data bagi memastikan pematuhan terhadap Prinsip-Prinsip Perlindungan Data Peribadi di bawah Akta Perlindungan Data Peribadi 2010 ("**Akta 709**").

1.2 Seksyen 5 Akta 709 memperuntukkan bahawa pemprosesan data peribadi oleh pengawal data hendaklah mematuhi Prinsip-Prinsip Perlindungan Data Peribadi, iaitu:

1.2.1 Prinsip Am;
1.2.2 Prinsip Notis dan Pilihan;
1.2.3 Prinsip Penzahiran;
1.2.4 Prinsip Keselamatan;
1.2.5 Prinsip Penyimpanan;
1.2.6 Prinsip Integriti Data; dan
1.2.7 Prinsip Akses

(secara kolektif, "**Prinsip-Prinsip PDP**").

Jika pemprosesan data peribadi dijalankan oleh pemproses data bagi pihak pengawal data, pemproses data tersebut hendaklah mematuhi Prinsip Keselamatan.

1.3 Penerapan pendekatan DPbD adalah penting bagi pengawal data dan pemproses data untuk beralih daripada minda yang reaktif kepada proaktif terhadap perlindungan data peribadi. Ia membantu memastikan pematuhan yang berkesan terhadap Akta 709, memperkukuh perlindungan hak subjek data serta memastikan kerangka perlindungan data peribadi Malaysia adalah relevan, berkesan dan selaras dengan landskap kawal selia perlindungan data global.

1.4 Garis Panduan ini menggariskan elemen panduan, aplikasi, ilustrasi dan amalan terbaik sebagai rujukan bagi pengawal data dan pemproses data mengenai cara pengaplikasian pendekatan DPbD. Garis Panduan ini tidak bersifat mandatori atau preskriptif. Pengawal data dan pemproses data digalakkan untuk menggunakan pendekatan berasaskan risiko dan menyesuaikan pelaksanaan DPbD berdasarkan sifat, saiz, skop, tujuan dan konteks aktiviti pemprosesan data masing-masing.

1.5 Garis Panduan ini dikaitkan dengan Standard Perlindungan Data Peribadi, Garis Panduan Pemberitahuan Pelanggaran Data, Garis Panduan Pemindahan Data Peribadi Rentas Sempadan serta Kod Tata Amalan yang dikeluarkan oleh atau yang didaftarkan dengan Pesuruhjaya Perlindungan Data Peribadi ("**Pesuruhjaya**"). Sebagai contoh, tindakan yang perlu diambil sekiranya berlaku insiden pelanggaran data peribadi adalah berkait rapat dengan panduan yang digariskan di bawah Garis Panduan Pemberitahuan Pelanggaran Data.

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

2. Peruntukan undang-undang

2.1 Garis Panduan ini dikeluarkan oleh Pesuruhjaya selaras dengan fungsi Pesuruhjaya di bawah subseksyen 48(g) Akta 709.

3. Tafsiran

3.1 Bagi maksud Garis Panduan ini, DPbD ditakrifkan seperti berikut:

> "Mereka Bentuk Berdasarkan Perlindungan Data" bermaksud suatu pendekatan yang menyepadukan langkah-langkah teknikal dan organisasi yang sewajarnya, yang direka untuk melaksanakan Prinsip-Prinsip PDP ke dalam seluruh kitaran hayat aktiviti pemprosesan data, bermula daripada reka bentuk, pembangunan dan pelaksanaan sehinggalah kepada pelupusan.

3.2 DPbD memerlukan penyepaduan langkah-langkah perlindungan data peribadi ke dalam reka bentuk dan pembangunan sesebuah projek, sistem, program, proses dan teknologi dari peringkat awal. Pertimbangan privasi hendaklah diambil kira secara lalai *(by default)* di semua peringkat operasi pemprosesan data dari permulaan sehingga akhir. Pengawal data dan pemproses data hendaklah mengamalkan pendekatan proaktif terhadap perlindungan data peribadi yang memberi fokus kepada usaha menjangka dan mencegah pelanggaran privasi dan bukannya sekadar bertindak balas selepas berlakunya isu perlindungan data.

Contoh amalan DPbD:

Pasukan pemasaran sesebuah organisasi menyenggara pangkalan data alamat e-mel pelanggan yang diproses bagi pelbagai tujuan seperti menghantar buletin pemasaran, memproses pesanan produk dan mengurus program kesetiaan.

Bagi mematuhi Prinsip Penyimpanan di bawah Akta 709, pasukan tersebut menggunakan fungsi pertanyaan *(query)* pangkalan data untuk mengenal pasti tarikh pengumpulan alamat e-mel dan menetapkan tempoh masa standard bagi menentukan bila alamat tersebut mungkin tidak lagi diperlukan. Alamat e-mel yang mencapai tamat tempoh yang ditetapkan akan ditandakan untuk semakan manual bagi menentukan sama ada ia perlu dipadamkan.

Pendekatan ini mewujudkan jurang dalam perlindungan data. Lama kelamaan, pasukan tersebut sukar untuk menjejaki tarikh dan tujuan setiap pengumpulan, mengakibatkan alamat e-mel disimpan lebih lama daripada yang diperlukan.

Dengan mengaplikasikan pendekatan DPbD, pasukan pemasaran tersebut mereka bentuk pangkalan data supaya setiap alamat e-mel ditetapkan tempoh penyimpanan yang sewajarnya secara automatik semasa kemasukan data. Sebaik sahaja tempoh penyimpanan tersebut tamat, alamat e-mel akan dipadamkan secara automatik atau sekurang-kurangnya disekat secara automatik daripada penggunaan lanjut sehingga semakan dilakukan.

BAHAGIAN B: ELEMEN-ELEMEN DPbD

4. Elemen-elemen DPbD

4.1 Garis Panduan ini menggariskan empat (4) elemen DPbD seperti berikut:

Elemen 1: Sifat proaktif *(Proactiveness)*;
Elemen 2: Perlindungan hujung-ke-hujung *(End-to-end protection)*;
Elemen 3: Ketelusan *(Transparency)*; dan
Elemen 4: Berpusatkan pengguna *(User-centricity)*.

4.2 **Sifat Proaktif** ***(Proactiveness)*** merupakan satu pendekatan yang menekankan usaha menjangka dan mencegah risiko privasi sebelum ia berlaku serta membangunkan proses secara aktif bagi mencegah pelanggaran data peribadi dan bukannya sekadar mengambil langkah reaktif apabila risiko tersebut timbul. Pendekatan ini melibatkan:

4.2.1 mewujudkan struktur tadbir urus dan memperuntukkan sumber yang mencukupi bagi menyokong pengurusan risiko data peribadi dalam organisasi; dan

4.2.2 mereka bentuk sistem pemprosesan data peribadi yang meminimumkan pengumpulan, penggunaan dan penyimpanan data peribadi ke tahap minimum yang diperlukan serta melindungi data peribadi secara lalai *(by default)*.

4.3 **Perlindungan hujung-ke-hujung** ***(end-to-end protection)*** merujuk kepada usaha untuk memastikan perlindungan data sepanjang keseluruhan kitaran hayat data peribadi yang terlibat. Setiap fasa iaitu pengumpulan, pemprosesan, penyimpanan dan pelupusan hendaklah mematuhi Prinsip-prinsip PDP.

4.4 **Ketelusan** ***(transparency)*** merujuk kepada pembuktian kebertanggungjawaban (akauntabiliti) dalam aktiviti pemprosesan data peribadi. Pengawal data dan pemproses data hendaklah bersifat terbuka dan jujur mengenai cara data peribadi dikendalikan serta bersedia untuk membuktikan pematuhan terhadap amalan yang telah dinyatakan.

4.5 **Berpusatkan pengguna** ***(user-centricity)*** merujuk kepada pengiktirafan bahawa data peribadi pada akhirnya adalah milik subjek data serta memberikan subjek data tersebut kawalan ke atas data peribadinya. Projek, produk, perkhidmatan, sistem dan proses hendaklah direka bentuk secara sedar berasaskan kepentingan serta keperluan subjek data yang mempunyai kepentingan mutlak terbesar dalam pengurusan data peribadinya sendiri.

BAHAGIAN C: DPbD BAGI PRINSIP AM

5. Prinsip Am

Seksyen 6 Akta 709 menggariskan Prinsip Am:

"

(1) Seseorang pengawal data tidak boleh—

(a) dalam hal data peribadi selain data peribadi sensitif, memproses data peribadi mengenai seorang subjek data melainkan jika subjek data itu telah memberikan persetujuannya bagi pemprosesan data peribadi itu; atau

(b) dalam hal data peribadi sensitif, memproses data peribadi sensitif mengenai seorang subjek data kecuali mengikut peruntukan seksyen 40.

(2) Walau apa pun perenggan (1)(a), seseorang pengawal data boleh memproses data peribadi mengenai seorang subjek data jika pemprosesan itu perlu-

(a) bagi melaksanakan sesuatu kontrak yang subjek data itu ialah suatu pihak kepadanya;

(b) bagi mengambil langkah atas permintaan subjek data itu dengan tujuan untuk membuat sesuatu kontrak;

(c) bagi mematuhi apa-apa obligasi undang-undang yang pengawal data itu merupakan subjek baginya, selain suatu obligasi yang dikenakan oleh sesuatu kontrak;

(d) bagi melindungi kepentingan vital subjek data itu;

(e) bagi mentadbirkan keadilan; atau

(f) bagi menjalankan apa-apa fungsi yang diberikan kepada mana-mana orang oleh atau di bawah mana-mana undang-undang.

(3) Data peribadi tidak boleh diproses melainkan jika-

(a) data peribadi itu diproses bagi maksud yang sah yang berhubungan secara langsung dengan aktiviti pengawal data itu;

(b) pemprosesan data peribadi itu perlu bagi atau berhubungan secara langsung dengan maksud itu; dan

(c) data peribadi itu adalah mencukupi tetapi tidak berlebihan berhubung dengan maksud itu."

5.1 Prinsip Am di bawah Akta 709 menghendaki pengawal data:

(a) mempunyai asas undang-undang yang sah (contoh: persetujuan, pelaksanaan kontrak, dll.) bagi pemprosesan data peribadi;

(b) hanya memproses data peribadi bagi maksud yang sah di sisi undang-undang yang berkaitan secara langsung dengan aktiviti pengawal data tersebut dan sekiranya perlu bagi atau berkaitan secara langsung dengan maksud tersebut; dan

(c) hanya memproses data peribadi yang mencukupi dan tidak berlebihan berhubung dengan maksud tersebut.

5.2 Pendekatan DPbD dalam pematuhan Prinsip Am menghendaki pengawal data untuk menerapkan pertimbangan privasi ke dalam reka bentuk operasi pemprosesan data bermula dari awal bagi memastikan bahawa operasi tersebut adalah sah, khusus bagi sesuatu maksud dan berpandukan keperluan yang berkaitan. Ini termasuk langkah-

langkah bagi memastikan pematuhan hujung ke hujung terhadap asas undang-undang serta maksud pemprosesan yang relevan secara lalai (*by default*).

5.3 Pendekatan DPbD dalam pematuhan Prinsip Am juga menghendaki pengawal data untuk menerapkan pertimbangan privasi terhadap data peribadi subjek data yang berumur di bawah lapan belas (18) tahun dengan memastikan persetujuan yang sah diperoleh bagi pihak subjek data tersebut. Persetujuan bagi pihak subjek data hendaklah diperoleh daripada ibu bapa, penjaga atau seseorang yang mempunyai tanggungjawab ibu bapa terhadap subjek data tersebut.

5.4 Konsep dan aplikasi berikut bertujuan untuk membimbing pelaksanaan DPbD dalam mematuhi Prinsip Am. Ia tidak bersifat preskriptif atau menyeluruh dan hendaklah disesuaikan oleh pengawal data berdasarkan profil risiko khusus[1] serta operasi pemprosesan data peribadi masing-masing.

(a) **Ketetapan Awal *(Predetermination)*:** Maksud dan asas undang-undang bagi pemprosesan hendaklah ditetapkan sebelum pemprosesan dilakukan. Penetapan tersebut hendaklah menjadi rujukan dalam mereka bentuk pemprosesan serta menetapkan had bagi pemprosesan tersebut.

(b) **Kekhususan *(Specificity)*:** Maksud pemprosesan hendaklah dinyatakan secara spesifik dan jelas.

(c) **Peminimuman data *(Data minimisation)*:** Sebelum memproses data peribadi, pengawal data hendaklah menilai sama ada pengumpulan dan penggunaan data peribadi tersebut benar-benar perlu bagi maksud yang diniatkan. Sekiranya maksud tersebut boleh dicapai dengan data peribadi yang lebih sedikit, data peribadi yang kurang terperinci atau data peribadi yang teragregat[2] atau tanpa perlu memproses data peribadi sama sekali, operasi pemprosesan sebegini hendaklah direka bentuk dengan sewajarnya.

Semasa pemprosesan, pengawal data hendaklah menyemak secara berkala sama ada data peribadi tersebut masih diperlukan. Sekiranya pengenalpastian individu tidak lagi diperlukan (contohnya, untuk analisis statistik), data peribadi tersebut hendaklah dipadamkan secara kekal atau dinyahnama *(anonymised)* dengan secepat yang dapat dilaksanakan.

(d) **Pembezaan *(Differentiation)*:** Asas undang-undang dan maksud yang digunakan bagi setiap aktiviti pemprosesan hendaklah dibezakan.

(e) **Keberkaitan *(Relevance)*:** Asas undang-undang yang tepat hendaklah terpakai bagi pemprosesan dan dikaitkan secara jelas dengan maksud pemprosesan tersebut. Data peribadi yang diproses hendaklah relevan dengan

[1] "Profil risiko khusus" merujuk kepada tahap atau sifat risiko kepada seseorang subjek data yang timbul daripada operasi pemprosesan tertentu seseorang pengawal data. Sebagai contoh, pengawal data dalam industri perkhidmatan kesihatan berkemungkinan mempunyai profil risiko khusus seperti pemprosesan rekod perubatan atau data biometrik berbanding dengan industri lain, di mana aplikasi DPbD oleh pengawal data tersebut akan memberi tumpuan kepada perlindungan terhadap kemudaratan reputasi atau kecurian identiti.

[2] "Data peribadi yang teragregat" merujuk kepada maklumat yang telah digabungkan dan dirumuskan supaya ia tidak lagi dapat dikaitkan dengan individu tertentu. Sebagai contoh, pengawal data boleh meminimumkan data peribadi dalam laporan sumber manusia dengan melaporkan petunjuk teragregat seperti purata gaji, penggunaan cuti dan kadar pusing ganti kakitangan tanpa menggunakan rekod individu.

pemprosesan yang berkenaan dan pengawal data hendaklah berupaya untuk membuktikan kerelevanan tersebut.

(f) **Keperluan *(Necessity)*:** Maksud pemprosesan akan menentukan data peribadi yang diperlukan. Setiap jenis data peribadi hendaklah dikumpul dan digunakan hanya apabila diperlukan bagi mencapai tujuan tersebut dan di mana maksud itu tidak boleh dicapai dengan cara lain yang munasabah.

(g) **Pengehadan *(Limitation)*:** Pengawal data hendaklah mengehadkan pengumpulan data peribadi kepada apa yang diperlukan bagi maksud yang diniatkan dan tidak boleh memproses data peribadi melangkaui maksud tersebut. Bagi mengurangkan risiko penyalahgunaan atau pengubahan maksud pemprosesan, pengawal data hendaklah melaksanakan langkah-langkah teknikal (termasuk pencincangan[3] dan penyulitan[4]) serta langkah-langkah organisasi (seperti dasar dan kawalan kontraktual) yang bersesuaian.

(h) **Semakan *(Review)*:** Semakan secara berkala hendaklah dijalankan bagi mengesahkan sama ada pemprosesan masih diperlukan bagi maksud asal data peribadi tersebut dikumpulkan.

(i) **Pemberhentian *(Cessation)*:** Sekiranya asas undang-undang atau maksud pemprosesan tidak lagi terpakai, pemprosesan tersebut hendaklah dihentikan dengan segera.

(j) **Pelarasan *(Adjustment)*:** Sekiranya terdapat perubahan asas undang-undang yang sah kepada pemprosesan, pemprosesan tersebut hendaklah diselaraskan mengikut asas undang-undang baharu yang berkaitan.

(k) **Pengagihan tanggungjawab *(Allocation of responsibility)*:** Sekiranya lebih daripada satu pihak terlibat dalam pemprosesan, pihak-pihak tersebut hendaklah menetapkan tanggungjawab masing-masing terhadap subjek data secara jelas dan telus serta merangka langkah-langkah pemprosesan mengikut pengagihan peranan tersebut.

(l) **Teknologi yang meningkatkan privasi *(Privacy-enhancing technologies – PET)*:** Pengawal data disyorkan untuk menggunakan teknologi yang terkini dan bersesuaian bagi tujuan peminimuman data *(data minimisation).*

(m) **Persetujuan *(Consent)*:** Di mana persetujuan merupakan asas undang-undang bagi pemprosesan, pengawal data hendaklah memastikan bahawa persetujuan tersebut diperoleh dengan sewajarnya. Operasi pemprosesan hendaklah memudahkan proses penarikan balik persetujuan selaras dengan Seksyen 38 Akta 709.

---

[3] "Pencincangan *(hashing)*" menerangkan sebuah proses satu hala untuk mengubah data input kepada satu nilai dengan kepanjangan atau saiz tetap. Sebagai contoh, melalui penggunaan algoritma pada sebuah laman sesawang, tindakan log masuk ke akaun menggunakan kata laluan akan mencetuskan sistem untuk membandingkan data input dengan nilai cincangan *(hash value)* yang disimpan dalam pangkalan data kata laluan. Sekiranya kedua-dua nilai tersebut sepadan, akses kepada akaun akan diberikan.

[4] "Penyulitan *(encryption)*" menerangkan proses penukaran teks yang boleh dibaca manusia kepada teks yang tidak dapat difahami. Proses ini lazimnya bersifat dua (2) hala, di mana data disulitkan oleh penghantar menggunakan suatu kekunci dan selepas diterima, penerima akan menyahsulit *(decrypt)* data tersebut menggunakan kekunci yang berasingan untuk mendapatkan semula data asal yang boleh dibaca.

Contoh 1:

Sebuah kafe berhasrat untuk melancarkan platform secara dalam talian yang mempunyai sistem pesanan, program kesetiaan pelanggan dan borang maklum balas. Sebelum melancarkan platform tersebut, kafe berkenaan menetapkan maksud bagi pemprosesan data peribadi iaitu:

(i) memproses pesanan;
(ii) memproses pembayaran;
(iii) memaklumkan pelanggan apabila pesanan sedia untuk diambil;
(iv) mengesahkan pelanggan yang betul mengambil pesanan;
(v) membolehkan ahli menikmati faedah keahlian termasuk ganjaran hari lahir;
(vi) mengumpul maklum balas daripada pelanggan; dan
(vii) menghantar e-mel pemasaran kepada pelanggan mengenai produk baharu dan promosi.

Kafe tersebut kemudiannya mengenal pasti data peribadi minimum yang diperlukan bagi maksud pemprosesan. Sebagai contoh, bagi mengehadkan data peribadi yang diperlukan untuk mengesahkan pelanggan yang betul mengambil pesanan, kafe tersebut mereka bentuk platform untuk menjana kod unik bagi setiap pesanan secara automatik, supaya pelanggan boleh menggunakan kod unik tersebut untuk membuat pengesahan diri semasa mengambil pesanan mereka.

Dalam mengambil kira senario kemungkinan di mana pelanggan kehilangan kod unik pesanan mereka, platform tersebut mengumpul data peribadi minimum yang lain, contohnya nama pertama dan nombor telefon, sebagai pengesahan sandaran. Bagi program kesetiaan pelanggan kafe tersebut, kafe hanya mengumpul butiran bulan lahir pelanggan (dan bukan tarikh lahir atau tahun lahir mereka), kerana ia berhasrat untuk menawarkan ganjaran hari lahir yang boleh ditebus pada bila-bila masa sepanjang bulan kelahiran pelanggan tersebut.

Kafe tersebut seterusnya mengenal pasti asas undang-undang yang boleh dipakai bagi setiap maksud pemprosesan.

Asas undang-undang	***Maksud***
Pelaksanaan kontrak yang mana subjek data merupakan suatu pihak	(i) Memproses pesanan (ii) Memproses pembayaran (iii) Memaklumkan pelanggan apabila pesanan sedia untuk diambil (iv) Mengesahkan pelanggan yang betul mengambil pesanan (v) Membolehkan ahli menikmati faedah keahlian, termasuk ganjaran hari lahir
Persetujuan	(i) Mengumpul maklum balas daripada pelanggan (ii) Menghantar e-mel pemasaran kepada pelanggan untuk produk baharu dan promosi

Kafe tersebut memastikan bahawa persetujuan yang berasingan diperoleh semasa mengumpul data peribadi pelanggan bagi mendapatkan maklum balas mengenai perkhidmatannya dan menghantar e-mel pemasaran kepada pelanggan. Pelanggan

diberikan opsyen untuk memilih masuk *(opt-in)* bagi menerima e-mel pemasaran dengan menandakan kotak semak *(checkbox)* semasa membuat pesanan. Secara lalai, kotak semak ini tidak ditandakan.

Pelanggan yang memberikan maklum balas melalui borang dalam talian di laman sesawang dimaklumkan agar berhati-hati semasa memasukkan data peribadi mereka dan diberikan pilihan untuk memberikan persetujuan bagi pemprosesan data peribadi tersebut melalui kotak semak. Secara lalai, kotak semak ini tidak ditandakan.

Kafe tersebut juga memastikan bahawa secara lalai *(default)*, hanya kuki yang benar-benar diperlukan sahaja diaktifkan pada platform dalam talian. Kuki tambahan hanya akan diaktifkan apabila pelanggan memberikan persetujuan bagi penggunaannya.

Contoh 2:

Sebuah syarikat telekomunikasi sedang membangunkan aplikasi mudah alih baharu yang membolehkan pelanggan menguruskan akaun mereka dan menerima tawaran yang diperibadikan, di samping membolehkan syarikat memantau penggunaan bagi tujuan analitik dalaman dan penambahbaikan perkhidmatan. Pada peringkat awal reka bentuk aplikasi, syarikat berkenaan mengenal pasti tujuan pemprosesan data peribadi dan menetapkan data peribadi minimum yang diperlukan dan asas undang-undang yang sah untuk pemprosesan data peribadi tersebut.

Maksud	***Langkah-langkah DPbD***
Pengurusan akaun dan pengebilan	Untuk membolehkan pelanggan log masuk untuk melihat butiran peribadi mereka, mengemas kini maklumat pengebilan, melihat bil dan sejarah pembayaran serta membuat pembayaran, aplikasi tersebut memproses data seperti nama pelanggan, nombor telefon bimbit, alamat fizikal, alamat e-mel dan maklumat pembayaran. Pemprosesan ini dianggap perlu untuk pelaksanaan kontrak kerana fungsi-fungsi ini penting bagi memenuhi kontrak perkhidmatan telekomunikasi dengan pelanggan.
Tawaran yang diperibadikan	Pada mulanya, bahagian pemasaran mencadangkan pengumpulan data lokasi terperinci dan sejarah pelayaran untuk menghasilkan tawaran yang sangat diperibadikan. Walau bagaimanapun, selaras dengan langkah peminimuman data, bahagian tersebut memutuskan bahawa cadangan ini adalah berlebihan. Sebaliknya, mereka menentukan bahawa tawaran boleh diperibadikan secara berkesan menggunakan data yang kurang intrusif, seperti pelan perkhidmatan semasa pelanggan, volum penggunaan data dan destinasi panggilan (kod negara sahaja). Bagi tujuan penghantaran tawaran yang diperibadikan, syarikat bergantung kepada persetujuan pelanggan. Aplikasi ini direka supaya pelanggan mesti memilih untuk ikut serta *(opt-in)* bagi tawaran pemasaran dan promosi dengan menandakan kotak semak yang tidak ditandakan secara lalai.

	Pelanggan boleh menarik balik persetujuan tersebut dengan mudah pada bila-bila masa melalui tetapan aplikasi.
Analisis dalaman dan penambahbaikan perkhidmatan	Syarikat mengambil maklum ketiadaan keperluan untuk menganalisis corak penggunaan individu yang dikaitkan dengan pengecam peribadi untuk tujuan analisis dalaman dan penambahbaikan perkhidmatan dan sebaliknya mengumpul data agregat (contoh: trend merentas segmen pelanggan yang luas).

5.5 Senarai semak berikut menetapkan pelbagai langkah yang bersifat tidak menyeluruh bagi mengaplikasikan pendekatan DPbD dalam mematuhi Prinsip Am:

	Senarai Semak Prinsip Am	Y/T
1.	**Ketetapan Awal.** Menetapkan tujuan dan asas undang-undang pemprosesan sebelum sebarang pemprosesan data peribadi dilakukan.	
2.	**Kekhususan.** Menentukan maksud pemprosesan secara terperinci dan spesifik yang mungkin.	
3.	**Peminimuman data.** Meminimumkan pengumpulan dan pemprosesan data peribadi kepada hanya apa yang benar-benar perlu untuk maksud yang telah dikenal pasti.	
4.	**Persetujuan.** Di mana persetujuan merupakan asas undang-undang, pastikan persetujuan diperoleh melalui mekanisme pilihan *(opt-in),* mudah ditarik balik dan tidak menggunakan bahasa yang mengelirukan atau kabur.	
5.	**Penilaian.** Menjalankan Penilaian Impak Perlindungan Data (DPIA) sebelum pemprosesan bagi mengenal pasti risiko terhadap data peribadi serta melaksanakan langkah mitigasi yang bersesuaian.	
6.	**Semakan.** Menjalankan semakan secara berkala sepanjang kitaran hayat data peribadi bagi mengesahkan sama ada pemprosesan masih diperlukan untuk tujuan data peribadi tersebut dikumpulkan, serta sama ada asas undang-undang masih terus terpakai.	

BAHAGIAN D: DPbD BAGI PRINSIP NOTIS DAN PILIHAN

6. Prinsip Notis dan Pilihan

Seksyen 7 Akta 709 menggariskan Prinsip Notis dan Pilihan:

"*Seseorang pengawal data hendaklah melalui notis bertulis memaklumkan seorang subjek data-*

(a) bahawa data peribadi subjek data itu sedang diproses oleh atau bagi pihak pengawal data itu, dan hendaklah memberikan perihalan data peribadi itu kepada subjek data itu;

(b) maksud yang baginya data peribadi itu sedang atau akan dikumpulkan dan diproses selanjutnya;

(c) apa-apa maklumat yang ada pada pengawal data itu tentang sumber data peribadi itu;

(d) hak subjek data itu untuk meminta akses kepada dan untuk meminta pembetulan terhadap data peribadi itu dan bagaimana untuk menghubungi pengawal data itu tentang apa-apa pertanyaan atau aduan berkenaan dengan data peribadi itu;

(e) golongan pihak ketiga yang kepadanya pengawal data menzahirkan atau boleh menzahirkan data peribadi itu;

(f) pilihan dan cara yang ditawarkan oleh pengawal data itu kepada subjek data bagi mengehadkan pemprosesan data peribadi, termasuklah data peribadi yang berhubungan dengan orang lain yang boleh dikenal pasti daripada data peribadi itu;

(g) sama ada wajib atau sukarela bagi subjek data untuk memberikan data peribadi itu; dan

(h) jika wajib bagi subjek data itu untuk memberikan data peribadi itu, akibat kepadanya jika dia tidak memberikan data peribadi itu.

(2) Notis di bawah subseksyen (1) hendaklah diberikan dengan secepat yang dapat dilaksanakan oleh pengawal data itu-

(a) apabila subjek data itu pertama kalinya diminta oleh pengawal data itu untuk memberikan data peribadinya;

(b) apabila pengawal data itu pertama kalinya mengumpul data peribadi subjek data itu; atau

(c) dalam mana-mana hal lain, sebelum pengawal data itu-

(i) menggunakan data peribadi subjek data itu bagi maksud selain maksud yang baginya data peribadi itu dikumpulkan; atau

(ii) menzahirkan data peribadi itu kepada pihak ketiga.

(3) *Suatu notis di bawah subseksyen (1) hendaklah dalam bahasa kebangsaan dan bahasa Inggeris, dan individu itu hendaklah diberi cara yang jelas dan mudah diakses untuk membuat pilihannya, jika perlu, dalam bahasa kebangsaan dan bahasa Inggeris.*"

6.1 Prinsip Notis dan Pilihan menghendaki pengawal data untuk bersikap jelas dan terbuka dengan subjek data tentang cara pengawal data mengumpul, menggunakan dan berkongsi data peribadi subjek data tersebut.

6.2 Konsep dan aplikasi berikut bertujuan untuk membimbing pelaksanaan DPbD dalam mematuhi Prinsip Notis dan Pilihan. Ia tidak bersifat preskriptif atau menyeluruh dan

hendaklah disesuaikan oleh pengawal data berdasarkan profil risiko khusus dan operasi pemprosesan data peribadi masing-masing.

(a) **Kejelasan *(Clarity)*:** Maklumat hendaklah disampaikan dalam bahasa yang jelas, mudah, ringkas serta mudah difahami.

(b) **Semantik *(Semantics)*:** Komunikasi hendaklah mempunyai makna yang jelas kepada subjek data yang berkenaan.

(c) **Kebolehcapaian *(Accessibility)*:** Maklumat hendaklah mudah dicapai oleh subjek data.

(d) **Kontekstual *(Contextual)*:** Maklumat hendaklah diberikan pada masa yang relevan serta dalam bentuk yang bersesuaian.

(e) **Keberkaitan *(Relevance)*:** Maklumat hendaklah relevan dan terpakai secara khusus bagi subjek data yang berkaitan.

(f) **Reka bentuk universal *(Universal design)*:** Maklumat hendaklah boleh diakses oleh setiap subjek data. Ini termasuklah penggunaan bahasa yang boleh dibaca mesin bagi memudahkan serta mengautomasikan kebolehbacaan dan kejelasan maklumat tersebut.

(g) **Boleh difahami *(Comprehensible)*:** Subjek data hendaklah mempunyai pemahaman yang sewajarnya mengenai jangkaan beliau berkenaan pemprosesan data peribadinya.

(h) **Berbilang saluran *(Multi-channel)*:** Mekanisme untuk melaksanakan hak subjek data hendaklah disediakan melalui pelbagai saluran dan media serta tidak terhad kepada bentuk teks sahaja bagi meningkatkan kebarangkalian maklumat tersebut disampaikan kepada subjek data secara berkesan.

(i) **Berlapisan *(Layered)*:** Maklumat hendaklah disusun secara berlapisan supaya wujud keseimbangan antara kelengkapan dan pemahaman, di samping mengambil kira jangkaan munasabah subjek data.

6.3 Pengawal data hendaklah mengelak daripada menggunakan pola reka bentuk yang memperdayakan pada antara muka memandangkan reka bentuk sedemikian boleh mengelirukan atau mempengaruhi subjek data untuk membuat pilihan yang tidak disengajakan atau pilihan lain yang berpotensi memudaratkan, terutamanya pilihan yang hanya memberi manfaat kepada pengawal data dan bukannya melindungi kepentingan terbaik subjek data.

6.4 Contoh pola reka bentuk yang memperdayakan yang hendaklah dielakkan termasuk:

(a) **Sarat maklumat *(Overloading)*:** Subjek data dibebankan dengan terlalu banyak permintaan, maklumat, opsyen atau kemungkinan untuk mendorong subjek data berkongsi lebih banyak data peribadi atau secara tidak sengaja membenarkan pemprosesan data peribadi yang bercanggah dengan jangkaannya.

Contoh: Sebuah laman sesawang meminta subjek data untuk mengklik empat (4) kotak timbul (pop-up) yang berbeza semata-mata untuk mengesahkan tetapan kuki beliau.

(b) **Melangkau *(Skipping)*:** Antara muka atau pelayaran pengguna direka sedemikian rupa supaya subjek data terlupa atau terlepas pandang aspek perlindungan data.

Contoh: Platform media sosial memerlukan subjek data untuk memberikan nombor telefon dan menetapkan tetapan keterlihatan nombor telefon kepada "Semua orang" secara lalai (default), sedangkan terdapat tetapan lain yang lebih melindungi privasi seperti "Tiada Sesiapa" dan "Kenalan Saya".

(c) **Perangsangan *(Stirring)*:** Gesaan atau dorongan tingkah laku atau visual digunakan untuk mempengaruhi keputusan subjek data. Perkara ini menjejaskan pilihan yang akan dibuat oleh subjek data dengan memanipulasi emosinya.

Contoh: Sebuah platform media sosial memaparkan mesej "Anda tidak akan lagi berhubung dengan rakan-rakan anda. Adakah anda pasti?" apabila subjek data cuba memadamkan akaunnya.

(d) **Menghalang *(Obstructing)*:** Antara muka menyukarkan atau mustahil bagi subjek data untuk memahami bagaimana data peribadi mereka diproses atau diuruskan.

Contoh: Kawalan privasi tidak disediakan di lokasi lazim seperti tetapan akaun, pengepala (header) atau pengaki (footer) laman sesawang, sebaliknya disembunyikan di bawah pelbagai langkah yang mengelirukan.

(e) **Tidak tetap *(Fickle)*:** Reka bentuk antara muka yang tidak konsisten dan tidak jelas sehingga menyukarkan subjek data untuk mengemudi kawalan dan maklumat perlindungan data peribadi.

Contoh: Pada kebiasaannya, warna merah digunakan untuk tindakan "Padam" atau "Batal". Namun, pada skrin kebenaran data, warna merah digunakan untuk butang "Benarkan Semua" bagi menarik perhatian dan mengelirukan subjek data

(f) **Dibiarkan tidak termaklum *(Left in the dark)*:** Maklumat atau kawalan perlindungan data peribadi disembunyikan atau kompleks, sehingga menyebabkan subjek data tidak pasti bagaimana data peribadinya diproses dan hak beliau terhadap data peribadi tersebut.

Contoh: Subjek data tidak dimaklumkan semasa memadamkan akaunnya bahawa sebahagian daripada data peribadi beliau akan tetap disimpan walaupun selepas akaun tersebut dipadamkan serta tempoh masa data peribadi akan disimpan.

Contoh:

Kafe memastikan bahawa pelanggan didorong ke arah notis perlindungan data peribadi (notis privasi) apabila mereka membuat pesanan atau mendaftar akaun keahlian. Notis perlindungan data peribadi (notis privasi) tersebut ditulis dalam bahasa yang jelas dan ringkas bagi memudahkan pelanggan memahami bagaimana data peribadi mereka diproses. Maklumat disediakan secara berlapisan, di mana perkara paling penting diketengahkan dan maklumat terperinci disediakan dengan mudah bagi menjelaskan lagi pelbagai butiran dan konsep yang digunakan

dalam notis perlindungan data peribadi (notis privasi). Notis tersebut disediakan dan dipaparkan pada semua halaman laman sesawang, supaya pelanggan sentiasa hanya memerlukan satu klik untuk mengakses maklumat tersebut.

6.5 Senarai semak berikut menetapkan pelbagai langkah yang tidak bersifat menyeluruh bagi mengaplikasikan pendekatan DPbD dalam mematuhi Prinsip Notis dan Pilihan*:*

	Senarai Semak Notis dan Prinsip Pilihan	Y/T
1.	**Reka bentuk berpusatkan pengguna.** Mereka bentuk sistem yang menghormati kepentingan subjek data melalui tetapan privasi secara lalai *(by default)* yang kukuh serta notis perlindungan data peribadi (notis privasi) yang mudah diakses dan ditempatkan di lokasi yang bersesuaian.	
2.	**Persetujuan.** Di mana persetujuan merupakan asas undang-undang, pastikan persetujuan diperoleh melalui mekanisme pilihan *(opt-in),* mudah ditarik balik dan tidak menggunakan bahasa yang mengelirukan atau kabur.	
3.	**Notis.** Menyediakan notis perlindungan data peribadi (notis privasi) dalam Bahasa Kebangsaan dan Bahasa Inggeris dengan menggunakan bahasa yang jelas dan mudah difahami serta memastikan notis tersebut mudah diakses dan jika berkenaan, disampaikan melalui pelbagai saluran atau media.	
4.	**Kawalan pengguna.** Memastikan mekanisme yang membolehkan subjek data melaksanakan haknya disediakan dalam bahasa yang jelas serta mudah, mudah diakses, sesuai dengan konteks dan jika berkenaan, disampaikan melalui pelbagai saluran atau media yang bersesuaian.	

BAHAGIAN E: DPbD BAGI PRINSIP PENZAHIRAN

7. Prinsip Penzahiran

Seksyen 8 Akta 709 menggariskan Prinsip Penzahiran:

"Tertakluk kepada seksyen 39, tiada data peribadi boleh, tanpa persetujuan subjek data, dizahirkan-

(a) bagi apa-apa maksud selain—
(i) maksud yang baginya data peribadi itu hendak dizahirkan pada masa pengumpulan data peribadi itu; atau
(ii) suatu maksud yang berhubungan secara langsung dengan maksud yang disebut dalam subperenggan (i); atau

(b) kepada mana-mana pihak selain pihak ketiga daripada golongan pihak ketiga yang dinyatakan dalam perenggan 7(1)(e).”

7.1 Prinsip Penzahiran menghendaki pengawal data untuk:

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

(b) hanya menzahirkan data peribadi bagi maksud asal yang dinyatakan semasa pengumpulan data peribadi tersebut; dan

(c) hanya menzahirkan data peribadi kepada kelas pihak ketiga yang dinyatakan dalam notis perlindungan data peribadi (notis privasi) yang diberikan kepada subjek data.

7.2 Konsep dan aplikasi berikut bertujuan untuk membimbing pelaksanaan DPbD dalam mematuhi Prinsip Penzahiran. Ia bersifat fleksibel dan hendaklah disesuaikan oleh pengawal data berdasarkan profil risiko khusus dan operasi pemprosesan data peribadi masing-masing.

(a) **Ketetapan Awal *(Predetermination)*:** Asas undang-undang penzahiran hendaklah ditetapkan sebelum sebarang penzahiran dilakukan. Asas undang-undang tersebut menjadi panduan dalam mereka bentuk proses penzahiran dan menetapkan had penzahiran.

(b) **Penghindaran data *(Data avoidance)*:** Pengawal data hendaklah mengelak penzahiran data peribadi sepenuhnya sekiranya maksud yang berkaitan boleh dicapai tanpa data tersebut. Data peribadi yang telah disamarkan *(pseudonymised)*[5] atau teragregat *(aggregated)* hendaklah digunakan sekiranya sesuai.

(c) **Pembezaan *(Differentiation)*:** Asas undang-undang dan maksud bagi setiap aktiviti penzahiran hendaklah dibezakan dengan jelas.

(d) **Kaitan *(Relevance)*:** Asas undang-undang yang sah hendaklah digunakan bagi setiap penzahiran dan dikaitkan secara jelas dengan maksud penzahiran tersebut. Pengawal data hendaklah berupaya membuktikan bahawa data peribadi yang dizahirkan adalah relevan dengan penzahiran tersebut.

(e) **Keperluan *(Necessity)*:** Maksud pemprosesan menentukan apakah data peribadi yang diperlukan untuk penzahiran. Setiap jenis data peribadi hendaklah perlu bagi maksud yang dinyatakan dan hanya boleh dizahirkan sekiranya tujuan tersebut tidak dapat dicapai melalui kaedah lain.

(f) **Semakan *(Review)*:** Semakan secara berkala hendaklah dijalankan untuk mengesahkan sama ada penzahiran tersebut masih diperlukan bagi maksud asal data peribadi itu dizahirkan.

(g) **Pemberhentian *(Cessation)*:** Data peribadi tidak boleh lagi dizahirkan sekiranya asas undang-undang serta maksud penzahiran tidak lagi terpakai. Langkah-langkah kawalan dan perlindungan hendaklah diwujudkan bagi memastikan pihak ketiga yang memproses data peribadi menghentikan

[5] Dalam konteks data peribadi, samaran (*pseudonym*) berfungsi sebagai pengenal pasti yang menggantikan identiti sebenar subjek data (contohnya, menukar nama penuh individu kepada 'Pelanggan001'). Ini membolehkan pengawal data menjalankan operasi dan menggunakan data tersebut tanpa mendedahkan identiti sebenar subjek data secara langsung.

pemprosesan serta memadamkan atau memusnahkan data peribadi tersebut secara kekal.

(h) **Pelarasan *(Adjustment)*:** Sekiranya terdapat perubahan asas undang-undang yang sah bagi penzahiran, penzahiran tersebut hendaklah diselaraskan mengikut asas undang-undang baharu tersebut.

(i) **Keselamatan *(Security)*:** Langkah-langkah teknikal termasuk pencincangan *(hashing)* dan penyulitan *(encryption)* serta langkah-langkah organisasi, seperti dasar-dasar dan kawalan kontraktual hendaklah disediakan untuk memastikan data peribadi dizahirkan dengan selamat.

Contoh 1:

Sebuah kafe memetakan aliran data untuk mengenal pasti jenis data peribadi yang akan dizahirkan kepada pihak ketiga. Ia mengesahkan bahawa terdapat asas undang-undang yang sah bagi penzahiran tersebut dan pelanggan telah dimaklumkan mengenainya. Semasa proses pengenalpastian ini, kafe tersebut menganalisis perkhidmatan yang diperincikan di dalam kontrak yang akan dimeterai dengan pemberi perkhidmatan sistem pesanan dalam talian. Jenis data peribadi yang dikenalpasti mungkin merangkumi nama, nombor telefon, pola pesanan dan butir pembayaran. Memandangkan data peribadi akan dizahirkan kepada pemberi perkhidmatan bagi tujuan penyelenggaraan sandaran dan log, kafe tersebut memastikan perjanjiannya dengan pemberi perkhidmatan menggariskan dengan jelas peranan dan tanggungjawab setiap pihak dalam mengendalikan data peribadi. Selain itu, perjanjian tersebut secara jelas membenarkan kafe untuk menjalankan audit untuk menentusahkan pematuhan pemberi perkhidmatan terhadap tanggungjawab tersebut.

Contoh 2:

Sebuah klinik pakar memetakan aliran data peribadinya bagi memastikan bahawa penzahiran maklumat pesakit, seperti rujukan kepada makmal luar atau syarikat insurans, adalah berdasarkan asas undang-undang yang jelas dan persetujuan pesakit. Had penzahiran diterapkan ke dalam reka bentuk sistem, yang hanya membenarkan data peribadi minimum yang diperlukan untuk dikongsi dan penyamaran *(pseudonymisation)* digunakan sekiranya pengecaman penuh tidak diperlukan. Pesakit dimaklumkan mengenai pihak ketiga di mana data peribadi mereka akan dizahirkan melalui notis perlindungan data peribadi (notis privasi) semasa pendaftaran.

Klinik tersebut menjalankan semakan berkala bagi menilai sama ada penzahiran tersebut masih perlu dan relevan dengan maksud asal. Sekiranya maksud penzahiran telah tamat, seperti selepas episod rawatan berakhir, perkongsian data peribadi akan dihentikan dan pihak ketiga diwajibkan dalam kontrak untuk memadamkan data peribadi dengan selamat. Semua penzahiran akan direkodkan (dilog), disulitkan dan ditadbir oleh perjanjian perkongsian data peribadi bagi memastikan kerahsiaan pesakit terpelihara di samping mengekalkan ketelusan dan akauntabiliti.

Contoh 3:

Sebuah syarikat pembuatan menggunakan penderia Internet Benda (IoT) dan sistem berasaskan awan untuk memantau kecekapan pengeluaran dan keadaan peralatan. Apabila menzahirkan data operasi kepada penyedia analitik pihak ketiga atau penyedia peralatan, syarikat memastikan bahawa hanya data yang disamarkan (*pseudonymised*) atau teragregat dikongsi melainkan data peribadi sangat diperlukan. Sempadan penzahiran ditakrifkan terlebih dahulu dan semua kontrak pihak ketiga termasuk klausa yang memerlukan pengendalian dan pemadaman data peribadi dijalankan dengan selamat sebaik sahaja tujuan dipenuhi.

Syarikat tersebut menyemak secara berkala aturan perkongsian data peribadinya bagi memastikan penzahiran kekal relevan dan diperlukan. Sekiranya hubungan dengan pemberi perkhidmatan berakhir atau asas undang-undang bagi penzahiran berubah, syarikat menghentikan pemindahan data peribadi dan menentusahkan bahawa data peribadi yang dikongsi sebelum ini dimusnahkan dengan selamat. Semua penzahiran adalah disulitkan dan direkodkan *(log)* dan pekerja dilatih untuk memahami had serta syarat di mana data peribadi beliau, seperti metrik prestasi pekerja atau log akses mungkin boleh dizahirkan.

7.3 Senarai semak berikut menetapkan pelbagai langkah yang tidak bersifat menyeluruh bagi mengaplikasikan pendekatan DPbD dalam mematuhi Prinsip Penzahiran*:*

	Senarai Semak Prinsip Penzahiran	Y/T
1.	**Ketetapan Awal.** Menetapkan maksud dan asas undang-undang penzahiran sebelum sebarang penzahiran data peribadi dilakukan.	
2.	**Pengabstrakan.** Jika maksud pemprosesan (contoh: untuk penyediaan statistik) tidak memerlukan set data peribadi akhir merujuk kepada subjek data yang dikenal pasti, nyahnama *(anonymise)* atau padamkan data peribadi tersebut sebaik sahaja pengenalpastian tidak lagi diperlukan.	
3.	**Keselamatan.** Melaksanakan langkah keselamatan teknikal untuk melindungi data peribadi (contoh: pencincangan *(hashing)* dan penyulitan *(encryption))* serta langkah organisasi (contoh: dasar dan obligasi kontrak) bagi memastikan data peribadi dikendalikan dan dizahirkan secara selamat.	
4.	**Persetujuan.** Di mana persetujuan merupakan asas undang-undang, pastikan persetujuan diperoleh melalui mekanisme pilihan *(opt-in),* mudah ditarik balik dan tidak menggunakan bahasa yang mengelirukan atau kabur.	
5.	**Semakan.** Menjalankan semakan secara berkala sepanjang kitaran hayat data peribadi bagi mengesahkan sama ada pemprosesan masih diperlukan untuk tujuan data peribadi tersebut dikumpulkan, serta sama ada asas undang-undang masih terus terpakai.	
6.	**Pengurusan pihak ketiga :** Memastikan pihak ketiga mempunyai langkah-langkah perlindungan data peribadi yang mencukupi melalui kontrak atau kaedah lain sebelum memindahkan data peribadi kepada pihak tersebut.	

BAHAGIAN F: DPbD BAGI PRINSIP KESELAMATAN

8. Prinsip Keselamatan

Seksyen 9 Akta 709 menggariskan Prinsip Keselamatan:
"

(1) Seseorang pengawal data dan seseorang pemproses data hendaklah, apabila memproses data peribadi, mengambil langkah yang praktikal untuk melindungi data peribadi itu daripada apa-apa kehilangan, salah guna, ubah suaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan dengan mengambil kira-

(a) sifat data peribadi itu dan kemudaratan akibat daripada kehilangan, salah guna, ubah suaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan itu;

(b) tempat atau lokasi di mana data peribadi itu disimpan;

(c) apa-apa langkah keselamatan yang digabungkan ke dalam apa-apa kelengkapan yang dalamnya data peribadi itu disimpan;

(d) langkah yang diambil untuk memastikan kebolehpercayaan, integriti dan kewibawaan personel yang mempunyai akses kepada data peribadi itu; dan

(e) langkah yang diambil bagi memastikan pemindahan selamat data peribadi itu.

(2) Jika pemprosesan data peribadi dijalankan oleh seorang pemproses data bagi pihak seorang pengawal data, pemproses data itu hendaklah, bagi maksud melindungi data peribadi itu daripada apa-apa kehilangan, salah guna, ubah suaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan-

(a) memberikan jaminan yang mencukupi berkenaan dengan langkah keselamatan teknikal dan organisasi yang mengawal pemprosesan yang akan dijalankan; dan

(b) mengambil langkah yang munasabah bagi memastikan pematuhan langkah itu."

8.1 Prinsip Keselamatan menghendaki pengawal data dan pemproses data mengambil langkah-langkah praktikal untuk melindungi data peribadi daripada sebarang kehilangan, salah guna, ubahsuaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan.

8.2 Pemproses data hendaklah memberi jaminan kepada pengawal data bahawa mereka mempunyai langkah-langkah keselamatan dan organisasi yang cukup kukuh untuk memproses data peribadi dan seterusnya mengambil langkah-langkah yang munasabah untuk mematuhi jaminan tersebut.

8.3 Konsep dan aplikasi berikut bertujuan untuk membimbing pelaksanaan DPbD dalam mematuhi Prinsip Keselamatan. Ia tidak bersifat preskriptif atau menyeluruh dan hendaklah disesuaikan oleh pengawal data dan pemproses data berdasarkan profil risiko khusus dan operasi pemprosesan data masing-masing.

(a) **Sistem pengurusan keselamatan maklumat *(Information security management system)*:** Mempunyai kaedah operasi untuk mengurus dasar dan prosedur keselamatan maklumat.

(b) **Analisis risiko *(Risk analysis)*:** Menilai risiko terhadap keselamatan data peribadi dengan mempertimbangkan potensi impak ke atas subjek data dan

melaksanakan langkah-langkah untuk menangani risiko yang dikenal pasti. Bagi tujuan penilaian risiko, "pemodelan ancaman" *(threat modelling)* serta analisis permukaan serangan *(attack surface analysis)* yang komprehensif dan sistematik terhadap reka bentuk perisian hendaklah dibangunkan dan dikekalkan. Ini bertujuan untuk mengurangkan vektor serangan serta menutup ruang eksploitasi terhadap titik lemah atau kerentanan sistem.

(c) **Mereka bentuk berdasarkan keselamatan *(Security by design)*:** Mempertimbangkan keperluan keselamatan seawal mungkin dalam reka bentuk dan pembangunan sistem serta laksanakan penyepaduan berterusan dan ujian yang berkaitan.

(d) **Penyenggaraan *(Maintenance)*:** Semak dan uji secara berkala perisian, perkakasan, sistem dan perkhidmatan untuk mengesan serta menangani kerentanan dalam sistem yang menyokong pemprosesan data peribadi.

(e) **Pengurusan kawalan akses *(Access control management)*:** Hanya kakitangan yang diberikan kuasa dan memerlukan akses kepada data peribadi bagi keperluan tugas hendaklah diberikan akses dan hak akses tersebut hendaklah dibezakan mengikut peranan.

(f) **Pengehadan akses *(Access limitation)*:** Pemprosesan data peribadi hendaklah direka bentuk bagi memastikan hanya bilangan minimum kakitangan mempunyai akses kepada data peribadi untuk melaksanakan tugas mereka.

(g) **Pengehadan akses (kandungan) *(Access limitation (content))*:** Bagi setiap operasi pemprosesan, akses hendaklah dihadkan kepada atribut khusus dalam set data peribadi yang diperlukan sahaja untuk melaksanakan operasi tersebut. Akses juga hendaklah dihadkan kepada data peribadi bagi subjek data yang berada dalam skop tanggungjawab kakitangan berkenaan sahaja.

(h) **Pengasingan akses *(Access segregation)*:** Pemprosesan data peribadi hendaklah direka bentuk supaya data peribadi diasingkan bagi memastikan tiada individu yang diberi kuasa mempunyai akses menyeluruh kepada semua data peribadi tanpa keperluan yang sah.

(i) **Pemindahan yang selamat *(Secure transfers)*:** Pemindahan data peribadi hendaklah dilindungi daripada sebarang akses yang tidak dibenarkan atau pengubahan yang tidak disengajakan.

(j) **Penyimpanan selamat *(Secure storage)*:** Penyimpanan data hendaklah selamat daripada akses dan pengubahan yang tidak dibenarkan. Prosedur hendaklah diwujudkan untuk menilai risiko penyimpanan secara berpusat atau teragih serta menentukan kategori data peribadi yang terlibat. Sesetengah data peribadi mungkin memerlukan langkah keselamatan tambahan atau pengasingan.

(k) **Penyamaran *(Pseudonymisation)*:** Data peribadi hendaklah disamarkan sebaik sahaja data tersebut tidak lagi diperlukan untuk pengenalpastian secara langsung sebagai langkah keselamatan untuk meminimumkan risiko pelanggaran data peribadi, contohnya menggunakan kaedah pencincangan atau penyulitan. Kekunci identiti hendaklah disimpan secara berasingan daripada data yang telah disamarkan.

(l) **Sandaran/log *(Backups/logs)*:** Semua sandaran dan log hendaklah disimpan setakat yang diperlukan bagi tujuan keselamatan maklumat. Jejak audit dan pemantauan peristiwa hendaklah dilaksanakan sebagai kawalan keselamatan yang rutin. Sandaran dan log hendaklah dilindungi daripada akses dan pengubahsuaian yang tidak dibenarkan atau tidak sengaja.

(m) **Pemulihan bencana/kesinambungan perniagaan *(Disaster recovery / business continuity)*:** Keperluan pemulihan bencana sistem maklumat dan kesinambungan perniagaan hendaklah diwujudkan bagi memastikan pemulihan dan kebolehsediaan data peribadi dalam tempoh yang sewajarnya.

(n) **Perlindungan mengikut risiko *(Protection according to risk)*:** Semua kategori data peribadi hendaklah dilindungi mengikut tahap risiko individu bagi setiap jenis data peribadi tersebut dan bukannya berdasarkan risiko pemprosesan data secara keseluruhan semata-mata.

(o) **Pengurusan tindak balas insiden keselamatan *(Security incident response management)*:** Mewujudkan rutin, prosedur serta sumber bagi mengesan, membendung, mengendalikan, melaporkan dan menyemak semula pelanggaran data peribadi secara sistematik.

(p) **Pengurusan insiden *(Incident management)*:** Mewujudkan proses bagi mengendalikan pelanggaran data peribadi bagi memperkukuhkan ketahanan sistem pemprosesan. Ini merangkumi prosedur untuk memberitahu Pesuruhjaya dan subjek data yang terkesan.

Contoh 1:

Sebuah kafe memastikan bahawa privasi diterapkan dalam sistem pesanan dalam talian. Data peribadi pelanggan disimpan dan diproses dalam sistem pangkalan data tersulit yang berasingan. Sebelum pelancaran sistem, penilaian risiko keselamatan siber dilakukan terhadap infrastruktur IT untuk memastikan ia berfungsi seperti yang diharapkan. Penilaian semula dijalankan secara berkala.

Contoh 2:

Firma perunding menerapkan keselamatan ke dalam pengurusan projek dan sistem libat urus pelanggan dengan melaksanakan sistem pengurusan keselamatan maklumat yang selaras dengan piawaian antarabangsa. Data pelanggan, seperti laporan kewangan, pelan strategik dan rekod sumber manusia, disimpan dalam repositori yang disulitkan dengan kawalan akses berbeza berdasarkan peranan projek. Semasa reka bentuk sistem, pemodelan ancaman *(threat modelling)* dijalankan bagi mengenal pasti potensi kerentanan dan ujian penembusan *(penetration testing)* secara berkala dilaksanakan untuk memastikan daya tahan yang berterusan.

Akses kepada data peribadi dihadkan secara ketat kepada perunding yang ditugaskan untuk projek spesifik, dengan pengsegmenan *(segmentation)* lanjut bagi menyekat akses kepada atribut data peribadi yang relevan sahaja. Pemindahan fail yang selamat dan komunikasi yang disulitkan digunakan untuk berinteraksi dengan pelanggan dan penyamaran *(pseudonymisation)* digunakan semasa menyediakan laporan penanda aras atau analisis. Firma tersebut menyenggara sandaran yang selamat, pelan kesinambungan perniagaan serta mempunyai protokol tindak balas

insiden yang didokumenkan bagi mengurus dan melaporkan pelanggaran data selaras dengan kewajipan Akta 709.

8.4 Senarai semak berikut menetapkan pelbagai langkah yang tidak bersifat menyeluruh bagi mengaplikasikan pendekatan DPbD dalam mematuhi Prinsip Keselamatan*:*

	Senarai Semak Prinsip Keselamatan	Y/T
1.	**Pemisahan.** Mewujudkan kawalan teknologi, dasar dan prosedur untuk mengelakkan penggabungan set data peribadi yang diperoleh daripada sumber yang berbeza yang lazimnya dikenali sebagai pengaitan data *(data linkages)*. Sebagai contoh, mengasingkan data peribadi yang diproses bagi tujuan yang berbeza dalam pangkalan data yang berasingan secara lalai *(by default).*	
2.	**Pengabstrakan.** Jika maksud pemprosesan (contoh: untuk penyediaan statistik) tidak memerlukan set data peribadi akhir merujuk kepada subjek data yang dikenal pasti, nyahnama *(anonymise)* atau padamkan data peribadi tersebut sebaik sahaja pengenalpastian tidak lagi diperlukan.	
3.	**Pengehadan akses.** Melaksanakan kawalan akses bagi memastikan akses kepada data hanya diberikan kepada pihak yang diberi kuasa dan mempunyai keperluan yang sah.	
4.	**Keselamatan.** Melaksanakan langkah-langkah keselamatan untuk melindungi data peribadi sepanjang kitaran hayatnya supaya semua data peribadi dikumpul, diproses, dipindahkan, disimpan dan dimusnahkan dengan cara yang selamat.	
5.	**Komitmen peringkat atasan.** Memastikan pengurusan tertinggi mengiktiraf bahawa perlindungan data peribadi boleh wujud seiring dengan kepentingan perniagaan yang sah, serta menetapkan komitmen yang jelas untuk menentukan dan menguatkuasakan piawaian perlindungan data peribadi yang tinggi.	
6.	**Kebertanggungjawaban.** Mewujudkan fungsi khusus dalam organisasi (contoh: Pegawai Perlindungan Data) yang bertanggungjawab untuk mendokumentasikan, menyampaikan, memantau dan melaksanakan semua dasar serta prosedur perlindungan data peribadi.	
7.	**Penilaian.** Menjalankan Penilaian Impak Perlindungan Data (DPIA) sebelum pemprosesan bagi mengenal pasti risiko terhadap data peribadi serta melaksanakan langkah mitigasi yang bersesuaian.	
8.	**Semakan.** Menjalankan semakan secara berkala sepanjang kitaran hayat data peribadi untuk mengesahkan sama ada pemprosesan masih diperlukan bagi maksud data peribadi tersebut dikumpulkan, serta sama ada asas undang-undang masih terus terpakai.	
9.	**Penilaian risiko dan audit :** Menjalankan penilaian risiko dan audit secara berkala untuk mengenal pasti sebarang potensi kelemahan serta jurang pematuhan.	

Senarai Semak Prinsip Keselamatan		Y/T
10.	**Pengurusan pihak ketiga :** Memastikan pihak ketiga mempunyai langkah-langkah perlindungan data peribadi yang mencukupi melalui kontrak atau kaedah lain sebelum memindahkan data peribadi kepada pihak tersebut.	
11.	**Pengurusan pelanggaran.** Mewujudkan prosedur dan sumber yang mencukupi untuk mengesan, membendung, mengendalikan, melaporkan serta mengambil pengajaran daripada pelanggaran data peribadi.	

BAHAGIAN G: DPbD BAGI PRINSIP PENYIMPANAN

9. Prinsip Penyimpanan

Seksyen 10 Akta 709 menggariskan Prinsip Penyimpanan:
"

(1) Data peribadi yang diproses bagi apa-apa maksud tidak boleh disimpan lebih lama daripada yang diperlukan bagi memenuhi maksud itu.

(2) *Menjadi kewajipan seorang pengawal data untuk mengambil segala langkah yang munasabah untuk memastikan bahawa segala data peribadi dimusnahkan atau dipadamkan secara kekal jika data peribadi itu tidak lagi dikehendaki bagi maksud yang baginya data peribadi itu hendak diproses.*"

9.1 Prinsip Penyimpanan menghendaki pengawal data untuk tidak menyimpan data peribadi lebih lama daripada yang diperlukan bagi memenuhi tujuan pemprosesan tersebut.

9.2 Konsep dan aplikasi berikut bertujuan untuk membimbing pelaksanaan DPbD dalam mematuhi Prinsip Penyimpanan. Ia tidak bersifat preskriptif atau menyeluruh dan hendaklah disesuaikan oleh pengawal data berdasarkan profil risiko khusus dan operasi pemprosesan data peribadi masing-masing.

(a) **Peminimuman data *(Data minimisation)*:** Apabila pemprosesan lanjut terhadap data peribadi dijalankan, pengawal data hendaklah membuat pertimbangan secara berkala sama ada data peribadi tersebut masih memadai, relevan dan diperlukan atau perlu dipadamkan. Jika tujuan pemprosesan tidak memerlukan set akhir data peribadi merujuk kepada subjek data yang dikenal pasti atau boleh dikenal pasti (contohnya bagi tujuan statistik), tetapi pemprosesan awal memerlukannya (contohnya sebelum data diagregatkan), maka pengawal data hendaklah memadamkan data peribadi secara kekal sebaik sahaja pengenalpastian tidak lagi diperlukan.

(b) **Pemadaman dan/atau penyahnamaan *(Deletion and/ or anonymisation)*:** Sekiranya data peribadi tidak atau tidak lagi diperlukan bagi maksud pemprosesan, data peribadi tersebut hendaklah dinyahnama *(anonymised)* dan/atau dipadam. Prosedur dalaman dan fungsi sistem yang jelas hendaklah dibangunkan bagi melaksanakan pemadaman dan/atau penyahnamaan tersebut.

(c) **Keberkesanan penyahnamaan / pemadaman *(Effectiveness of anonymisation/ deletion)*:** Pengawal data hendaklah memastikan bahawa data yang dinyahnama *(anonymised)* tidak boleh dikenalpasti semula atau data yang dipadam tidak boleh dipulihkan. Pengawal data hendaklah menguji bagi memastikan tiada kemungkinan untuk pengenalpastian semula atau pemulihan data tersebut berlaku.

(d) **Automasi (Automation):** Pemadaman data peribadi tertentu hendaklah dilaksanakan secara automatik.

(e) **Kriteria penyimpanan *(Retention criteria)*:** Pengawal data hendaklah menentukan data peribadi dan tempoh penyimpanan yang diperlukan.

(f) **Justifikasi *(Justification)*:** Pengawal data hendaklah berupaya memberikan justifikasi mengapa tempoh penyimpanan yang ditetapkan diperlukan serta rasional tempoh penyimpanan tersebut, termasuk asas undang-undangnya.

(g) **Penguatkuasaan dasar penyimpanan *(Enforcement of retention policies)*:** Pengawal data hendaklah menguatkuasakan dasar penyimpanan dalaman dan menjalankan ujian bagi memastikan polisi tersebut dikuatkuasakan dengan sewajarnya.

(h) **Sandaran/log *(Backups/logs)*:** Pengawal data hendaklah menentukan jenis data peribadi dan tempoh penyimpanan yang diperlukan bagi tujuan sandaran dan log.

(i) **Aliran data *(Data flow)*:** Pengawal data hendaklah menyedari aliran data peribadi serta penyimpanan sebarang salinannya dan berusaha untuk mengehadkan penyimpanan sementara data tersebut. Aliran data peribadi hendaklah diuruskan dengan cekap supaya tidak mewujudkan lebih banyak salinan daripada yang diperlukan.

Contoh 1:

Pangkalan data yang menyimpan data peribadi pelanggan direka bentuk supaya tempoh penyimpanan setiap data peribadi dijana secara automatik sebaik sahaja tersebut dimasukkan ke dalam pangkalan data. Data peribadi yang telah tamat tempoh simpanannya akan dipadamkan secara automatik.

Contoh 2:

Sebuah platform media sosial tempatan mengumpul kandungan yang dihasilkan oleh pengguna[6], data lokasi dan analisis tingkah laku untuk menyesuaikan paparan *(feeds)* serta menyiarkan iklan bersasar. Platform ini menguatkuasakan peraturan penyimpanan data peribadi yang jelas, contohnya memadamkan akaun yang dinyahaktifkan dan data peribadi yang berkaitan selepas tempoh yang ditetapkan. Apabila subjek data memadamkan hantaran atau mesej, data peribadi tersebut dipadamkan secara selamat daripada sistem aktif dan juga sandaran. Data peribadi yang dikongsi dengan pengiklan diagregatkan dan dinyahnama *(anonymised)* bagi

[6] Kandungan digital seperti teks, imej, video atau audio yang dihasilkan oleh pengguna platform media sosial.

memastikan subjek data tersebut tidak boleh dikenal pasti semula, sementara masih membolehkan analisis perniagaan dijalankan.

9.3 Senarai semak berikut menetapkan pelbagai langkah yang tidak bersifat menyeluruh bagi mengaplikasikan pendekatan DPbD dalam mematuhi Prinsip Penyimpanan:

	Senarai Semak Prinsip Penyimpanan	Y/T
1.	**Peminimuman data.** Meminimumkan pengumpulan dan pemprosesan data peribadi kepada hanya apa yang benar-benar perlu untuk maksud yang telah dikenal pasti.	
2.	**Pengabstrakan.** Jika maksud pemprosesan (contoh: untuk penyediaan statistik) tidak memerlukan set data peribadi akhir merujuk kepada subjek data yang dikenal pasti, nyahnama *(anonymise)* atau padamkan data peribadi tersebut sebaik sahaja pengenalpastian tidak lagi diperlukan.	
3.	**Pengehadan akses.** Melaksanakan kawalan akses bagi memastikan akses kepada data hanya diberikan kepada pihak yang diberi kuasa dan mempunyai keperluan yang sah.	
4.	**Keselamatan.** Melaksanakan langkah-langkah keselamatan untuk melindungi data peribadi sepanjang kitaran hayatnya supaya semua data peribadi dikumpul, diproses, dipindahkan, disimpan dan dimusnahkan dengan cara yang selamat.	

BAHAGIAN H: DPbD BAGI PRINSIP INTEGRITI DATA

10. Prinsip Integriti Data

Seksyen 11 Akta 709 menggariskan Prinsip Integriti Data:

"*Seseorang pengawal data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini dengan mengambil kira maksud, termasuk apa-apa maksud yang berhubungan secara langsung, yang baginya data peribadi itu dikumpulkan dan diproses selanjutnya.*"

10.1 Prinsip Integriti Data menghendaki pengawal data mengambil langkah-langkah yang munasabah untuk memastikan bahawa data peribadi adalah tepat, lengkap, tidak mengelirukan dan sentiasa dikemas kini dengan mengambil kira maksud data peribadi tersebut dikumpulkan serta diproses selanjutnya.

10.2 Pendekatan DPbD dalam mematuhi Prinsip Integriti Data selanjutnya menghendaki pengawal data untuk mengambil langkah-langkah yang munasabah bagi data peribadi subjek data di bawah umur lapan belas (18) tahun. Ini termasuk memastikan penyumberan dan pembetulan data peribadi tersebut boleh diakses dengan mudah diakses oleh ibu bapa, penjaga atau orang yang mempunyai tanggungjawab ibu bapa terhadap subjek data tersebut.

10.3 Konsep dan aplikasi berikut bertujuan untuk membimbing pelaksanaan DPbD dalam mematuhi Prinsip Integriti Data. Ia tidak bersifat preskriptif atau menyeluruh dan hendaklah disesuaikan oleh pengawal data berdasarkan profil risiko khusus dan operasi pemprosesan data peribadi masing-masing.

(a) **Sumber data *(Data source)*:** Data peribadi hendaklah diperoleh daripada sumber yang boleh dipercayai untuk memastikan ketepatan data peribadi.

(b) **Tahap ketepatan *(Degree of accuracy)***: Setiap elemen data peribadi hendaklah setepat yang diperlukan bagi maksud yang ditetapkan.

(c) **Rekod boleh dikait *(Attributable recording)*:** Pengawal data hendaklah mempunyai rekod yang boleh mengenalpasti bila dan sebab kakitangan atau sistem memasukkan data peribadi semasa peringkat penyumberan.

(d) **Pengesahan *(Verification)*:** Bergantung pada sifat data peribadi dan kekerapan perubahan data tersebut, pengawal data hendaklah mengesahkan ketepatan data peribadi dengan subjek data sebelum dan pada pelbagai peringkat pemprosesan (contohnya, keperluan pengesahan apabila mencapai umur persaraan).

(e) **Pembetulan *(Rectification)*:** Pengawal data hendaklah memudahkan urusan pembetulan data yang tidak tepat tanpa kelengahan apabila diminta oleh subjek data.

(f) **Pencegahan penyebaran ralat *(Error-propagation avoidance)*:** Pengawal data hendaklah mengurangkan kesan ralat terkumpul dalam rantaian pemprosesan.

(g) **Akses *(Access)*:** Subjek data hendaklah dibekalkan dengan maklumat dan diberikan akses yang berkesan kepada data peribadinya selaras dengan Prinsip Akses bagi memastikan ketepatan serta membolehkan pembetulan dilakukan mengikut keperluan.

(h) **Ketepatan berterusan *(Continued accuracy)*:** Data peribadi hendaklah tepat pada setiap peringkat pemprosesan dan ujian ketepatan hendaklah dijalankan pada langkah-langkah pemprosesan yang kritikal.

(i) **Dikemas kini *(Up-to-date)*:** Data peribadi hendaklah dikemas kini sekiranya perlu bagi maksud pemprosesan tersebut.

(j) **Reka bentuk data *(Data design)*:** Pengawal data hendaklah menggunakan ciri-ciri reka bentuk teknologi dan organisasi untuk meminimumkan ketidaktepatan, contohnya dengan menyediakan pilihan pratentu yang ringkas *(predetermined choices)* berbanding medan teks bebas *(free-text fields).*

Contoh:

Sebuah syarikat teknologi kewangan *(Fintech)* menawarkan platform untuk pinjaman peribadi. Bagi memastikan integriti data peribadi, syarikat melaksanakan sistem yang kukuh untuk mengesahkan ketepatan maklumat pelanggan memandangkan integriti data peribadi adalah kritikal bagi penilaian risiko kredit yang tepat dan penyaluran pinjaman. Apabila pelanggan memohon pinjaman, syarikat menggunakan proses pengesahan "kenali pelanggan anda" (KYC) pada platform tersebut yang merujuk silang data peribadi yang diberikan (nama, nombor kad

pengenalan, alamat) dengan pangkalan data Kerajaan dan kewangan yang boleh dipercayai. Ini berfungsi sebagai pengesahan sumber data peribadi utama bagi mengurangkan risiko ralat.

Syarikat tersebut juga membangunkan ciri-ciri untuk memudahkan ketepatan data yang dipacu oleh pengguna. Semasa proses permohonan, platform memaparkan ringkasan maklumat yang diberikan dan meminta pengguna untuk menyemak serta mengesahkan ketepatannya sebelum penghantaran, sekaligus memberi peluang untuk pembetulan. Bagi data peribadi yang bersifat dinamik seperti alamat kediaman pemohon, sistem turut merangkumi peringatan pengesahan berkala. Sebagai contoh, enam (6) bulan selepas pinjaman dikeluarkan, pelanggan menerima pemberitahuan untuk mengesahkan sama ada alamat atau butiran hubungan mereka masih terkini bagi memastikan data peribadi kekal tepat untuk komunikasi berterusan dan pengurusan akaun.

Selain itu, sistem dalaman syarikat direka bentuk untuk menghalang penyebaran ralat. Sebarang perubahan pada data peribadi pelanggan, sama ada dimulakan oleh pelanggan atau kakitangan syarikat, akan melalui semakan pengesahan automatik sebelum disimpan ke dalam pangkalan data berpusat. Ini memastikan sebarang ketidaktepatan dikesan pada peringkat kemasukan dan tidak dibawa ke dalam proses lain yang berkaitan, seperti model pemarkahan kredit atau arahan pengeluaran. Pendekatan ini melindungi integriti data peribadi sepanjang kitaran hayatnya, daripada pengumpulan hingga pemprosesan, sekaligus melindungi syarikat daripada risiko kewangan serta pelanggan daripada menerima perkhidmatan yang mengelirukan atau tidak tepat.

10.4 Senarai semak berikut menetapkan pelbagai langkah tidak menyeluruh bagi mengaplikasikan pendekatan DPbD dalam mematuhi Prinsip Integriti Data:

	Prinsip Integriti Data	Y/T
1.	**Kebolehcapaian.** Menyediakan mekanisme yang membolehkan subjek data mengakses data peribadinya dengan mudah.	
2.	**Reka bentuk data.** Menggunakan ciri-ciri reka bentuk teknologi dan organisasi untuk meminimumkan ketidaktepatan, contohnya dengan menyediakan pilihan pratentu yang ringkas *(predetermined choices)* berbanding medan teks bebas *(free-text fields)*.	
3.	**Kawalan pengguna.** Memastikan mekanisme yang membolehkan subjek data melaksanakan haknya disediakan dalam bahasa yang jelas serta mudah, mudah diakses, sesuai dengan konteks dan jika berkenaan, disampaikan melalui pelbagai saluran atau media yang bersesuaian.	
4.	**Pembetulan**. Memudahkan pembetulan data peribadi yang tidak tepat tanpa kelewatan selepas menerima permintaan daripada subjek data.	
5.	**Semakan.** Menjalankan ujian ketepatan data peribadi secara berkala.	

BAHAGIAN I: DPbD BAGI PRINSIP AKSES

11. Prinsip Akses

Seksyen 12 Akta 709 menggariskan Prinsip Akses:

"*Seseorang subjek data hendaklah diberi akses kepada data peribadinya yang dipegang oleh seorang pengawal data dan boleh membetulkan data peribadi itu jika data peribadi itu tidak tepat, tidak lengkap, mengelirukan atau tidak terkini, kecuali jika pematuhan dengan permintaan untuk akses atau pembetulan itu enggan diberikan di bawah Akta ini.*"

11.1 Prinsip Akses menghendaki pengawal data membenarkan subjek data mengakses data peribadi mereka serta membetulkan data yang tidak tepat, tidak lengkap, mengelirukan atau tidak terkini selepas menerima permintaan pembetulan menurut Seksyen 34 Akta 709. Subjek data hendaklah dimaklumkan mengenai pihak yang perlu dihubungi bagi mengemukakan permintaan tersebut. Maklumat hubungan hendaklah mudah diakses serta ditempatkan di lokasi yang strategik, contohnya dalam akaun pengguna, maklumat kontekstual (contohnya maklumat yang dipaparkan semasa penggunaan perkhidmatan), notis perlindungan data peribadi (notis privasi), soalan lazim (FAQ) dan saluran lain yang bersesuaian.

11.2 Pendekatan DPbD dalam mematuhi Prinsip Akses selanjutnya menghendaki pengawal data untuk mereka bentuk sistem yang sesuai bagi data peribadi milik subjek data di bawah umur lapan belas (18) tahun. Sistem sedemikian hendaklah memastikan data peribadi tersebut boleh diakses dengan mudah oleh ibu bapa, penjaga atau orang yang mempunyai tanggungjawab ibu bapa terhadap subjek data tersebut.

11.3 Konsep dan aplikasi berikut bertujuan untuk membimbing pelaksanaan DPbD dalam mematuhi Prinsip Akses. Ia tidak bersifat preskriptif atau menyeluruh dan hendaklah disesuaikan oleh pengawal data berdasarkan profil risiko khusus dan operasi pemprosesan data peribadi masing-masing.

(a) **Kejelasan *(Clarity)*:** Maklumat tentang cara melaksanakan hak subjek data hendaklah disediakan dalam bahasa yang jelas, mudah, ringkas dan boleh difahami.

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

(c) **Kontekstual *(Contextual)*:** Mekanisme untuk melaksanakan hak subjek data hendaklah disediakan pada masa yang berkaitan dan dalam bentuk yang sesuai.

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

(e) **Boleh difahami *(Comprehensible)*:** Subjek data hendaklah mempunyai pemahaman yang sewajarnya terhadap jangkaan mereka berkenaan sejauh mana mereka boleh melaksanakan hak data peribadi tersebut.

(f) **Berbilang saluran *(Multi-channel)*:** Mekanisme untuk melaksanakan hak subjek data hendaklah disediakan melalui pelbagai saluran dan media, serta tidak terhad kepada bentuk teks sahaja, bagi meningkatkan kebarangkalian maklumat tersebut disampaikan kepada subjek data secara berkesan.

Contoh:

Pihak kafe memastikan pelanggan dapat melaksanakan hak terhadap data peribadi mereka dengan mudah. Di dalam profil akaun masing-masing, terdapat pilihan akses pantas bagi pelanggan untuk memuat turun data peribadi dalam format yang boleh diakses, mengemas kini data atau memadam akaun. Pelanggan akan dimaklumkan dengan segera mengenai penerimaan permintaan tersebut serta cara menjejaki status permintaan sehingga ke peringkat pengesahan. Selain itu, butiran hubungan turut diberikan sekiranya pelanggan memerlukan sokongan lanjut.

11.4 Senarai semak berikut menetapkan pelbagai langkah tidak menyeluruh bagi mengaplikasikan pendekatan DPbD dalam mematuhi Prinsip Akses:

	Senarai Semak Prinsip Akses	Y/T
1.	**Kebolehcapaian.** Menyediakan mekanisme yang membolehkan subjek data mengakses data peribadinya dengan mudah.	
2.	**Reka bentuk berpusatkan pengguna.** Mereka bentuk sistem yang menghormati kepentingan subjek data melalui tetapan privasi secara lalai *(by default)* yang kukuh serta notis perlindungan data peribadi (notis privasi) yang mudah diakses dan ditempatkan di lokasi yang bersesuaian.	
3.	**Kawalan pengguna.** Memastikan mekanisme yang membolehkan subjek data melaksanakan haknya disediakan dalam bahasa yang jelas serta mudah, mudah diakses, sesuai dengan konteks dan jika berkenaan, disampaikan melalui pelbagai saluran atau media yang bersesuaian.	

12. Senarai semak

12.1 Satu senarai semak telah dibangunkan untuk membimbing pelaksanaan pendekatan DPbD. Senarai semak di **Lampiran A**, menggariskan langkah-langkah pelaksanaan DPbD yang bersifat tidak menyeluruh *(non-exhaustive)* dan disusun kepada dua (2) kategori berikut:

(a) **Langkah-langkah Berorientasikan Data *(Data-Oriented Measures)*:** memfokuskan kepada aspek teknikal dalam pemprosesan data; dan

(b) **Langkah-langkah Berorientasikan Proses *(Process-Oriented Measures)*:** memfokuskan kepada aspek organisasi dan prosedur dalam pemprosesan data.

BAHAGIAN J: AMALAN TERBAIK BAGI TADBIR URUS DPbD

13. Amalan terbaik

13.1 DPbD adalah mengenai mewujudkan budaya organisasi yang mengamalkan pendekatan berasaskan prinsip dan proaktif terhadap pengurusan data peribadi. Pendekatan ini hendaklah diterapkan di seluruh organisasi serta dicerminkan dalam produk, perkhidmatan, tadbir urus dan operasinya. Ini hendaklah melibatkan:

(a) komitmen yang jelas daripada pengurusan kanan untuk menetapkan dan menguatkuasakan piawaian perlindungan data yang tinggi;

(b) pemupukan budaya di mana semua pihak berkepentingan berkongsi komitmen terhadap penambahbaikan berterusan dalam piawaian perlindungan data; dan

(c) pewujudan proses untuk mengenalpasti jurang dalam reka bentuk serta amalan semasa dan menangani isu secara proaktif dan sistematik sebelum ia berlaku.

13.2 Ilustrasi berikut menggariskan amalan terbaik bagi pelaksanaan tadbir urus DPbD. Ia tidak bersifat mandatori dan bertujuan untuk membimbing organisasi, yang mana mereka digalakkan untuk mengaplikasikannya mengikut pendekatan berasaskan risiko yang selaras dengan profil risiko dan konteks operasi masing-masing.

(a) Memastikan komitmen kepimpinan kanan serta penyertaan aktif mereka dalam mewujudkan kerangka perlindungan data peribadi yang kukuh dan proaktif dalam organisasi, antaranya melalui:

(i) memastikan terdapat ahli Lembaga Pengarah yang mempunyai kepakaran dalam perlindungan data atau memastikan pengarah menerima latihan yang sewajarnya dalam bidang tersebut;

(ii) memastikan para pengarah memperuntukkan sumber yang mencukupi bagi langkah-langkah DPbD, termasuk untuk penambahbaikan teknologi;

(iii) melantik sekurang-kurangnya seorang pengurus kanan atau Ketua Jabatan untuk bertanggungjawab ke atas pematuhan data peribadi organisasi;

(iv) memasukkan pematuhan perlindungan data peribadi sebagai sebahagian daripada penilaian prestasi pengurusan kanan;

(v) mewajibkan penilaian dan audit data peribadi dijalankan dan dilaporkan kepada Lembaga Pengarah secara berkala;

(vi) mengadakan mesyuarat secara berkala dengan Pegawai Perlindungan Data (DPO) organisasi, jika berkenaan.

(b) Menjalankan audit secara berkala terhadap dasar perlindungan data peribadi untuk mengesahkan keberkesanan pelaksanaannya secara praktikal serta pematuhan operasi.

(c) Membangunkan kaedah sistematik termasuk Penilaian Impak Perlindungan Data (DPIA) untuk mengenalpasti dan menilai risiko bagi memastikan sebarang impak negatif dikurangkan sebelum ia berlaku.

(d) Memupuk budaya dan persekitaran di mana semua pihak berkepentingan termasuk pengguna digalakkan untuk mencadangkan penambahbaikan terhadap amalan perlindungan data serta memastikan cadangan tersebut disemak secara sistematik dan diterima pakai dengan sewajarnya.

LAMPIRAN A: SENARAI SEMAK LANGKAH-LANGKAH BERORIENTASIKAN DATA DAN BERORIENTASIKAN PROSES

	Langkah-langkah Berorientasikan Data	Y/T
1.	**Ketetapan Awal.** Menetapkan maksud dan asas undang-undang pemprosesan sebelum pemprosesan dimulakan.	
2.	**Kekhususan.** Menentukan maksud pemprosesan secara terperinci dan spesifik setakat yang mungkin.	
3.	**Peminimuman data.** Meminimumkan pengumpulan dan pemprosesan data peribadi kepada hanya apa yang benar-benar perlu untuk maksud yang telah dikenal pasti.	
4.	**Pemisahan.** Mewujudkan kawalan teknologi, dasar dan prosedur untuk mengelakkan penggabungan set data peribadi yang diperoleh daripada sumber yang berbeza yang lazimnya dikenali sebagai pengaitan data *(data linkages)*. Sebagai contoh, mengasingkan data peribadi yang diproses bagi tujuan yang berbeza dalam pangkalan data yang berasingan secara lalai *(by default).*	
5.	**Pengabstrakan.** Jika maksud pemprosesan (contoh: untuk penyediaan statistik) tidak memerlukan set data peribadi akhir merujuk kepada subjek data yang dikenal pasti, nyahnama *(anonymise)* atau padamkan data peribadi tersebut sebaik sahaja pengenalpastian tidak lagi diperlukan.	
6.	**Pengehadan akses.** Melaksanakan kawalan akses bagi memastikan akses kepada data hanya diberikan kepada pihak yang diberi kuasa dan mempunyai keperluan yang sah.	
7.	**Keselamatan.** Melaksanakan langkah-langkah keselamatan untuk melindungi data peribadi sepanjang kitaran hayatnya supaya semua data peribadi dikumpul, diproses, dipindahkan, disimpan dan dimusnahkan dengan cara yang selamat.	
8.	**Reka bentuk berpusatkan pengguna.** Mereka bentuk sistem yang menghormati kepentingan subjek data melalui tetapan privasi secara lalai *(by default)* yang kukuh serta notis perlindungan data peribadi (notis privasi) yang mudah diakses dan ditempatkan di lokasi yang bersesuaian.	
	Langkah-langkah Berorientasikan Proses	
9.	**Persetujuan.** Di mana persetujuan merupakan asas undang-undang, pastikan persetujuan diperoleh melalui mekanisme pilihan *(opt-in),* mudah ditarik balik dan tidak menggunakan bahasa yang mengelirukan atau kabur.	
10.	**Notis.** Menyediakan notis perlindungan data peribadi (notis privasi) dalam Bahasa Kebangsaan dan Bahasa Inggeris dengan menggunakan bahasa yang jelas dan mudah difahami serta memastikan notis tersebut mudah diakses dan, jika berkenaan, disampaikan melalui pelbagai saluran atau media.	

11.	**Kawalan pengguna.** Memastikan mekanisme yang membolehkan subjek data melaksanakan haknya disediakan dalam bahasa yang jelas serta mudah, mudah diakses, sesuai dengan konteks dan jika berkenaan, disampaikan melalui pelbagai saluran atau media yang bersesuaian.	
12.	**Komitmen peringkat atasan.** Memastikan pengurusan tertinggi mengiktiraf bahawa perlindungan data peribadi boleh wujud seiring dengan kepentingan perniagaan yang sah, serta menetapkan komitmen yang jelas untuk menentukan dan menguatkuasakan piawaian perlindungan data peribadi yang tinggi.	
13.	**Kebertanggungjawaban.** Mewujudkan fungsi khusus dalam organisasi (contoh: Pegawai Perlindungan Data) yang bertanggungjawab untuk mendokumentasikan, menyampaikan, memantau dan melaksanakan semua dasar serta prosedur perlindungan data peribadi.	
14.	**Penilaian.** Menjalankan Penilaian Impak Perlindungan Data (DPIA) sebelum pemprosesan bagi mengenal pasti risiko terhadap data peribadi serta melaksanakan langkah mitigasi yang bersesuaian.	
15.	**Semakan.** Menjalankan semakan secara berkala sepanjang kitaran hayat data peribadi untuk mengesahkan sama ada pemprosesan masih diperlukan bagi maksud data peribadi tersebut dikumpulkan, serta sama ada asas undang-undang masih terus terpakai.	
16.	**Penilaian risiko dan audit :** Menjalankan penilaian risiko dan audit secara berkala untuk mengenal pasti sebarang potensi kelemahan serta jurang pematuhan.	
17.	**Pengurusan pihak ketiga :** Memastikan pihak ketiga mempunyai langkah-langkah perlindungan data peribadi yang mencukupi melalui kontrak atau kaedah lain sebelum memindahkan data peribadi kepada pihak tersebut.	
18.	**Pengurusan pelanggaran.** Mewujudkan prosedur dan sumber yang mencukupi untuk mengesan, membendung, mengendalikan, melaporkan serta mengambil pengajaran daripada pelanggaran data peribadi.	