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.	

MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION
GUIDELINE

DATA PROTECTION BY DESIGN (DPbD)

Version 1.0
Date of Issuance: 30 April 2026

DEPARTMENT OF PERSONAL DATA PROTECTION

Address:

DEPARTMENT OF PERSONAL DATA PROTECTION
Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana
Precinct 4, Federal Government Administration Centre
62100 Putrajaya, Malaysia

TABLE OF CONTENTS

PART A: INTRODUCTION

1. Background

1.1 This Data Protection by Design Guideline ("**Guideline**") sets out guidance on applying the Data Protection by Design ("DPbD") approach to the data controller and data processor to ensure compliance with the Personal Data Protection Principles under the Personal Data Protection Act 2010 ("**Act 709**").

1.2 Section 5 of the Act 709 provides that the processing of personal data by a data controller shall comply with the Personal Data Protection Principles, which are:

1.2.1 General Principle;
1.2.2 Notice and Choice Principle;
1.2.3 Disclosure Principle;
1.2.4 Security Principle;
1.2.5 Retention Principle;
1.2.6 Data Integrity Principle; and
1.2.7 Access Principle

(collectively, "**PDP Principles**").

Where the processing of personal data is carried out by a data processor on behalf of the data controller, the data processor shall comply with the Security Principle.

1.3 The adoption of a DPbD approach is essential for the data controller and data processor to shift from a reactive to a proactive mindset towards personal data protection. It helps to ensure effective compliance with Act 709, strengthens protection of the data subject's rights and ensures that Malaysia's personal data protection framework is relevant, effective and aligned with the global data protection regulatory landscape.

1.4 This Guideline sets out guiding elements, applications, illustrations and best practices as a reference for the data controller and the data processor on how to apply the DPbD approach. It is not intended to be mandatory or prescriptive. The data controller and data processor are encouraged to apply a risk-based approach and tailor the DPbD efforts based on the nature, size, scope, purposes and context of the data processing activities.

1.5 This Guideline is linked to the Personal Data Protection Standard, Data Breach Notification Guideline, Cross-Border Personal Data Transfer Guideline and the Codes of Practice issued by or registered with the Personal Data Protection Commissioner ("**Commissioner**"). For example, actions to be taken in the event of a personal data breach are closely related to the guidance set out under the Data Breach Notification Guideline.

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

2. Legal provisions

2.1 This Guideline is issued by the Commissioner pursuant to the functions of the Commissioner under subsection 48(g) of the Act 709.

3. Interpretation

3.1 For the purposes of this Guideline, DPbD is defined as follows:

> "Data protection by design" means an approach that incorporates appropriate technical and organisational measures, which are designed to implement the PDP Principles, into the entire lifecycle of a data processing activity, from design, development and deployment to decommissioning.

3.2 DPbD requires the incorporation of personal data protection measures into the design and development of projects, systems, programmes, processes and technologies from the outset. Privacy considerations shall be taken into account at all stages of a data processing operation, by default, from the beginning to the end. The data controller and the data processor shall adopt a proactive stance to personal data protection that focuses on anticipating and preventing privacy breaches, rather than merely reacting after data protection issues have occurred.

Example of DPbD in practice:

An organisation's marketing team maintains a database of customers' email addresses processed for different purposes, such as sending marketing newsletters, processing product orders and managing loyalty programmes.

To comply with the Retention Principle under Act 709, the team creates a database query to identify the collection dates of the email addresses and applies a standard timeframe to determine when the addresses may no longer be needed. Email addresses reaching the set expiry are flagged for manual review to decide on deletion.

This approach creates gaps in data protection. Over time, the team struggles to track the date and purpose of each collection, resulting in email addresses being retained for longer than necessary.

By applying a DPbD approach, the marketing team designs the database so that each email address is automatically assigned an appropriate retention period upon entry. Once the retention period ends, the email address is automatically deleted, or at a minimum, automatically blocked from further use until it is reviewed.

PART B: DPbD ELEMENTS

4. Elements of DPbD

4.1 This Guideline outlines four (4) DPbD elements, which are as follows:

Element 1: Proactiveness;
Element 2: End-to-end protection;
Element 3: Transparency; and
Element 4: User-centricity.

4.2 **Proactiveness** is an approach that emphasises anticipating and preventing privacy risks before they occur, as well as actively developing processes to prevent personal data breaches, rather than merely taking reactive measures when such risks arise. This approach involves:

4.2.1 establishing governance arrangements and allocating adequate resources to support personal data risk management within the organisation; and

4.2.2 designing the personal data processing systems that minimise the collection, use and retention of personal data to the minimum extent necessary, and protecting personal data by default.

4.3 **End-to-end protection** refers to ensuring data protection throughout the entire lifecycle of the personal data involved. Every phase, namely collection, processing, storage and disposal shall comply with the PDP Principles.

4.4 **Transparency** refers to demonstrating accountability in personal data processing activities. The data controller and data processor shall be open and honest about how the personal data is handled and be prepared to demonstrate compliance with the stated practices.

4.5 **User-centricity** refers to recognising that personal data ultimately belongs to the data subject and giving the data subject control over his personal data. Projects, products, services, systems and processes shall be consciously designed around the interests and needs of the data subject, who has the greatest vested interest in the management of his own personal data.

PART C: DPbD FOR GENERAL PRINCIPLE

5. General Principle

Section 6 of Act 709 outlines the General Principle:

"

(1) A data controller shall not-

(a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or

(b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of section 40.

(2) Notwithstanding paragraph (1)(a), a data controller may process personal data about a data subject if the processing is necessary-

(a) for the performance of a contract to which the data subject is a party;

(b) for the taking of steps at the request of the data subject with a view to entering into a contract;

(c) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;

(d) in order to protect the vital interests of the data subject;

(e) for the administration of justice; or

(f) for the exercise of any functions conferred on any person by or under any law.

(3) Personal data shall not be processed unless-

(a) the personal data is processed for a lawful purpose directly related to an activity of the data controller;

(b) the processing of the personal data is necessary for or directly related to that purpose; and

(c) the personal data is adequate but not excessive in relation to that purpose."

5.1 The General Principle under the Act 709 requires that the data controller:

(a) has a valid legal basis (e.g. consent, performance of a contract, etc.) for the processing of personal data;

(b) only process personal data for a lawful purpose directly related to the data controller's activity and where necessary for or directly related to the purpose; and

(c) only process personal data that is adequate but not excessive in relation to the purpose.

5.2 A DPbD approach in compliance with the General Principle requires the data controller to embed privacy considerations into the design of the data processing operation to ensure, from the outset that the data processing operation is valid, purpose-specific and guided by necessity, with measures that ensure end-to-end adherence to the relevant legal bases and purposes of processing by default.

5.3 A DPbD approach in compliance with the General Principle further requires the data controller to embed privacy considerations into the personal data of the data subject aged under eighteen (18) years, including ensuring that valid consent is obtained on behalf of the data subject. Such consent shall be obtained from the parent, guardian or person who has parental responsibility for that data subject.

5.4 The following concepts and applications are intended to guide the implementation of DPbD in complying with the General Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile[1] and the personal data processing operations.

(a) **Pre-determination:** The purpose and the legal basis of processing shall be established before the processing takes place. These shall guide the design of the processing and set the processing boundaries.

(b) **Specificity:** The purposes of processing shall be specified and explicit.

(c) **Data minimisation:** Before processing personal data, the data controller shall assess whether collecting and using the personal data are truly necessary for the intended purpose. Where the purpose can be achieved with less data, less detailed or aggregated personal data[2] or without using personal data at all, the processing shall be designed accordingly.

During processing, the data controller shall regularly review whether the personal data remains necessary. Where identification of individuals is no longer required (for example, for statistical analysis), the personal data shall be permanently deleted or anonymised as soon as practicable.

(d) **Differentiation:** The legal basis and purpose used for each processing activity shall be differentiated.

(e) **Relevance:** The correct legal basis shall be applied to the processing and clearly connected to the specific purpose of processing. The personal data processed shall be relevant to the processing in question, and the data controller shall be able to demonstrate this relevance.

(f) **Necessity:** The purpose of processing determines what personal data is required. Each type of personal data shall be collected and used only where it is necessary to achieve that purpose and where the purpose cannot reasonably be achieved by other means.

(g) **Limitation:** The data controller shall limit the collection of personal data to what is necessary for its intended purpose and shall not process personal data beyond such intended purpose. To reduce the risk of misuse or repurposing,

[1] "Specific risk profile" refers to the level and nature of risks to a data subject arising from a data controller's particular processing operation. As an example, a data controller in the healthcare services industry may have a specific risk profile such as the processing of medical records or biometric data, as compared to other industries, whereby a data controller's application of DPbD will be focused on safeguarding against reputational harm or identity theft.

[2] "Aggregated personal data" refers to information that has been combined and summarised so that it can no longer be linked to a specific individual. For example, a data controller may minimise personal data in a human resources report by reporting aggregated indicators such as average salary, leave utilisation, and staff turnover rates rather than using individual records.

the data controller shall implement appropriate technical measures (including hashing[3] and encryption[4]) and organisational measures (such as policies and contractual controls).

(h) **Review:** Regular reviews shall be conducted to verify whether the processing is necessary for the purposes for which the personal data was collected.

(i) **Cessation:** If the legal basis or purpose for processing no longer applies, the processing must cease immediately.

(j) **Adjustment:** If there is a valid change of legal basis for the processing, the actual processing shall be adjusted in accordance with the new legal basis.

(k) **Allocation of responsibility:** If multiple parties are involved in the processing, the parties shall clearly and transparently define their respective responsibilities toward the data subject and design the processing measures according to this division of roles.

(l) **Privacy-enhancing technologies (PETs):** The data controller is recommended to apply up-to-date and appropriate technologies for data minimisation.

(m) **Consent:** Where consent is the legal basis for processing, the data controller shall ensure that consent is properly obtained. The processing operation shall facilitate the withdrawal of consent process in accordance with section 38 of Act 709.

Example 1:

A café intends to launch an online platform with an ordering system, customer loyalty programme and feedback form. Before launching the platform, the café determines the purposes for processing personal data, which are to:

(i) process orders;
(ii) process payments;
(iii) notify customers when their order is ready for pickup;
(iv) verify that the correct customer is picking up the order;
(v) allow for membership benefits, including birthday rewards;
(vi) collect feedback from customers; and
(vii) send customers marketing emails about new products and promotions.

The café then identifies the minimum personal data required for the purposes of processing. For example, to limit the personal data required to verify that the correct customer is picking up an order, the café designs the platform to automatically generate a unique code for each order, so that customers can use the unique code to identify themselves when picking up their order.

[3] "Hashing" describes a one-way process to transform input data into a value of fixed length or size. For example, through the use of an algorithm on a website, logging into the website account through a password will trigger the system to compare the input data with a stored hash value in the password database. the two values match, access to the account will be granted.

[4] "Encryption" describes a process of converting human-readable text into incomprehensible text. The process is usually two-way, encryption of data is performed using a key by the sender, and upon receipt, the receiver decrypts using a separate key to recover the original human-readable data.

To account for the likely scenario where customers lose the unique code to their order, the platform collects other minimum personal data, e.g. first name and phone number, as fallback identifiers. For the café's customer loyalty programme, the café only collects the customers' birth month (and not their birth date or birth year), as it intends to offer birthday rewards that are redeemable any time during the customer's birth month.

The café then identifies the legal bases which can be relied upon for each purpose of processing.

Legal basis	*Purpose*
Performance of a contract to which the data subject is a party	(i) Process orders (ii) Process payments (iii) Notify customers when their order is ready for pickup (iv) Verify that the correct customer is picking up the order (v) Allow members to enjoy membership benefits, including birthday rewards
Consent	(i) Collect feedback from customers to improve service (ii) Send customers marketing emails about new products and promotions

The café makes sure that a separate consent is obtained when it collects personal data from customers to collect feedback about its service and to send marketing emails to customers. Customers are given the option to opt-in by ticking a checkbox to receive marketing emails when they make an order. This checkbox is by default unchecked.

Customers providing feedback via the website's online feedback form are notified to be cautious about including their personal data in the feedback form and to opt-in by ticking a checkbox to consent to the processing of the personal data that they provide in the feedback form. The checkbox is by default unchecked.

The café also ensures that by default, only the strictly necessary cookies used by the online platform are active. The additional cookies are activated only when the customer consents to their use.

Example 2:

A telecommunications company is developing a new mobile application that allows customers to manage their accounts and receive personalised offers and allows the company to monitor usage for internal analytics and service improvement. In the beginning stages of designing the app, the company identifies the purposes for processing personal data and determines the minimum personal data required and valid legal bases for processing the personal data.

Purpose	***DPbD measures***
Account management and billing	To allow customers to log in, view their personal details, update their billing information, view their bills and payment

	history and make payments, the app processes data such as a customer's name, mobile number, physical address, email address, and payment information. This is deemed necessary for the performance of the contract as these functions are integral to fulfilling the telecommunications service contract with a customer.
Personalised offers	Initially, the marketing team proposed collecting detailed location data and browsing history to create highly personalised offers. However, following the data minimisation measure, the team decides that this is excessive. Instead, they determine that offers can be effectively personalized using less intrusive data, such as a customer's current service plan, data usage volume, and call destinations (country code only). For the purpose of sending personalised offers, the company relies on customer consent. The app is designed so that customers must opt in for marketing and promotional offers by ticking a checkbox which is unchecked by default. Customers can easily withdraw their consent at any time through the app's settings.
Internal analytics and service improvement	The company notes that it is not necessary to analyse individual usage patterns linked to personal identifiers for purposes of internal analytics and service improvement and collects aggregated data (e.g. trends across broad customer segments) instead.

5.5 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the General Principle:

	General Principle Checklist	Y/N
1.	**Predetermination.** Establish the purposes and the legal basis for processing before any personal data processing takes place.	
2.	**Specificity.** Define the purpose(s) for processing as narrowly and specifically as possible.	
3.	**Data minimisation.** Minimise the collection and processing of personal data to what is strictly necessary for the identified purpose(s).	

General Principle Checklist		Y/N
4.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
5.	**Assessment.** Conduct a Data Protection Impact Assessment (DPIA) before the processing to identify personal data risks and implement appropriate mitigation measures.	
6.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	

PART D: DPbD FOR NOTICE AND CHOICE PRINCIPLE

6. Notice and Choice Principle

Section 7 of Act 709 outlines the Notice and Choice Principle:

"

(1) A data controller shall by written notice inform a data subject-

- *(a) that personal data of the data subject is being processed by or on behalf of the data controller, and shall provide a description of the personal data to that data subject;*
- *(b) the purposes for which the personal data is being or is to be collected and further processed;*
- *(c) of any information available to the data controller as to the source of that personal data;*
- *(d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data controller with any inquiries or complaints in respect of the personal data;*
- *(e) of the class of third parties to whom the data controller discloses or may disclose the personal data;*
- *(f) of the choices and means the data controller offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;*
- *(g) whether it is obligatory or voluntary for the data subject to supply the personal data; and*
- *(h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.*

(2) The notice under subsection (1) shall be given as soon as practicable by the data controller-

- *(a) when the data subject is first asked by the data controller to provide his personal data;*
- *(b) when the data controller first collects the personal data of the data subject; or*
- *(c) in any other case, before the data controller-*

(i) uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or
(ii) discloses the personal data to a third party.

(3) A notice under subsection (1) shall be in the national and English languages, and the individual shall be provided with a clear and readily accessible means to exercise his choice, where necessary, in the national and English languages."

6.1 The Notice and Choice Principle requires the data controller to be clear and open with the data subject about how the data controller collects, uses and share the data subject's personal data.

6.2 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Notice and Choice Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile and personal data processing operations.

(a) **Clarity:** Information shall be provided in clear, plain, concise and intelligible language.

(b) **Semantics:** Communication shall have a clear meaning to the data subject in question.

(c) **Accessibility:** Information shall be easily accessible to the data subject.

(d) **Contextual:** Information shall be provided at the relevant time and in the appropriate form.

(e) **Relevance:** Information shall be relevant and applicable to the specific data subject.

(f) **Universal design:** Information shall be accessible to the data subject. This includes the use of machine-readable languages to facilitate and automate the readability and clarity of the information.

(g) **Comprehensible:** The data subject shall have a fair understanding of what he can expect with regard to the processing of his personal data.

(h) **Multi-channel:** Information shall be provided through various channels and media, not limited to textual forms, to increase the likelihood of the information reaching the data subject effectively.

(i) **Layered:** Information shall be layered in a manner that balances completeness and understanding, while accounting for the data subject's reasonable expectations.

6.3 The data controller shall refrain from the use of deceptive design patterns in interfaces as these designs may mislead or pressure the data subject into making unintended or into making otherwise potentially harmful choices, especially those that benefit the data controller instead of protecting the data subject's best interests.

6.4 Examples of deceptive design patterns that shall be avoided include:

(a) **Overloading:** The data subject is presented with too many requests, information, options or possibilities in order to prompt the data subject to share more personal data or unintentionally allow personal data processing against the data subject's expectations.

Example: A website asks the data subject to click through four (4) different pop-up boxes just to confirm the cookie settings.

(b) **Skipping:** The interface or user journey is designed so that the data subject forgets or overlooks the data protection aspects.

Example: A social media platform requires the data subject to provide a phone number and sets the phone number's visibility setting to "Everybody" by default, even when there are other more privacy-protective settings like "Nobody" and "My Contacts".

(c) **Stirring:** Behavioural or visual prompts or nudges are used to influence the data subject's decisions. This affects the choice the data subject would make by manipulating his emotions.

Example: A social media platform displays the message "You will no longer stay connected with your friends. Are you sure?" when the data subject attempts to delete his account.

(d) **Obstructing:** The interface makes it difficult or impossible for the data subject to understand how the personal data is processed or managed.

Example: Privacy controls are not made available in standard locations such as the account settings or the website header or footer but concealed under multiple confusing steps.

(e) **Fickle:** The design of the interface is inconsistent and unclear, making it hard for the data subject to navigate different personal data protection controls and information.

Example: Usually, the red colour is used for "Delete" or "Cancel" action. However, on the data permission screen, red colour is suddenly used for the "Allow All" button to attract the attention and to confuse the data subject.

(f) **Left in the dark:** Personal data protection information or controls are hidden or complicated, causing the data subject unsure of how his personal data is processed and the rights he has over his personal data.

Example: The data subject is not informed when deleting his account that some of his personal data will still be retained even after the account is deleted, as well as the period for which the personal data will be stored.

Example:

The café ensures that customers are directed to the personal data protection notice (privacy notice) when they make an order or create a membership account. The personal data protection notice (privacy notice) is written in clear and concise language to make it easy for the customers to understand how the personal data is processed. The information is provided in a layered manner, where the most

important points are highlighted and detailed information is made easily available to further explain the various items and concepts used in the personal data protection (privacy notice). The personal data protection notice (privacy notice) is made available and is visible on all web pages of the website, so that the customer is always only one click away from accessing the information.

6.5 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Notice and Choice Principle*:*

	Notice and Choice Principle Checklist	Y/N
1.	**User-centred design.** Design systems that respect the data subject's interests through robust default privacy settings, easily accessible personal data protection notices (privacy notices) and appropriate user-friendly privacy management tools.	
2.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
3.	**Notice.** Provide a personal data protection notice (privacy notice) in both the National Language and English, using clear and plain language and ensure that the notice is easily accessible and, where applicable, communicated through multiple channels or media.	
4.	**User Control**: Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	

PART E: DPbD FOR DISCLOSURE PRINCIPLE

7. Disclosure Principle

Section 8 of Act 709 outlines the Disclosure Principle:

"

Subject to section 39, no personal data shall, without the consent of the data subject, be disclosed-

(a) for any purpose other than-

(i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or

(ii) a purpose directly related to the purpose referred to in subparagraph (i); or

(b) *to any party other than a third party of the class of third parties as specified in paragraph 7(1)(e)*."

7.1 The Disclosure Principle requires that the data controller:

(a) obtain the data subject's consent or otherwise have a valid legal basis for the disclosure of personal data;

(b) only disclose personal data for the purpose for which the personal data was to be disclosed at the time of collection of the personal data; and

(c) only disclose personal data to the class of third parties specified in the personal data protection (privacy notice) provided to the data subject.

7.2 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Disclosure Principle. They are meant to be flexible and may be adjusted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Predetermination:** The legal basis of disclosure shall be established prior to any disclosure. Such legal basis shall guide the design of the disclosure process and set the disclosure boundaries.

(b) **Data avoidance:** The data controller shall avoid disclosing personal data altogether whenever possible for the relevant purpose. Pseudonymised[5] or aggregated personal data shall be used when feasible.

(c) **Differentiation:** The legal basis and purpose used for each disclosure activity shall be clearly differentiated.

(d) **Relevance:** The valid legal basis shall be applied to each disclosure and shall be clearly connected to the specific purpose of disclosure. The data controller shall be able to demonstrate that the personal data disclosed is relevant to that disclosure.

(e) **Necessity:** The purpose determines what personal data is necessary for the disclosure. Each personal data type shall be necessary for the specified purposes and shall only be disclosed if it is not possible to fulfil the purpose by other means.

(f) **Review:** Regular reviews shall be conducted to verify whether the disclosure remains necessary for the purposes for which the personal data was disclosed.

(g) **Cessation:** Personal data shall no longer be disclosed if the legal basis and purpose of disclosure cease to apply. Measures and safeguards shall be in place to ensure that the third party ceases processing and permanently deletes or destroys the personal data.

[5] In a personal data context, a pseudonym serves as an identifier replacing a data subject's actual identity (e.g., changing an individual's full name to 'Customer001'). This enables the data controller to perform operations and use the data without directly revealing the data subject's identity.

(h) **Adjustment:** If there is a valid change of legal basis for the disclosure, the disclosure shall be adjusted in accordance with the new legal basis.

(i) **Security:** Technical measures, including hashing and encryption, and organisational measures, such as policies and contractual obligations shall be in place to ensure that personal data is disclosed securely.

Example 1:

The café maps its data flows to identify the types of personal data that will be disclosed to third parties. It confirms that there is a legal basis for such disclosure and that customers have been informed accordingly. During the identification process, the café reviews the services specified in the contract with the online ordering system vendor.

The types of personal data may include name, phone number, ordering patterns, and payment details. Since personal data will be disclosed to the vendor for purposes of maintaining back-ups and logs, the café ensures that its agreement with the vendor clearly outlines the roles and responsibilities of each party in handling personal data. Furthermore, the agreement explicitly allows the café to conduct audits to verify the vendor's compliance with those responsibilities.

Example 2:

A specialist clinic maps its personal data flows to ensure that disclosures of patient information, such as referrals to external laboratories or insurers, are based on clearly defined legal grounds and patient consent. Disclosure boundaries are embedded into system design, allowing only the minimum necessary personal data to be shared, and pseudonymisation is applied where full identifiers are not required. Patients are informed of the third parties to whom their personal data may be disclosed through a personal data protection notice (privacy notice) during registration.

The clinic conducts regular reviews to assess whether ongoing disclosures remain necessary and relevant to the original purpose. If a disclosure purpose expires, such as after a treatment episode ends, personal data sharing is ceased and third parties are contractually required to securely delete the personal data. All disclosures are logged, encrypted and governed by personal data-sharing agreements ensuring that patient confidentiality is preserved while maintaining transparency and accountability.

Example 3:

A manufacturing company uses Internet-of-Things (IoT) sensors and cloud-based systems to monitor production efficiency and equipment condition. When disclosing operational data to third-party analytics providers or equipment vendors, the company ensures that only pseudonymised or aggregated data is shared unless personal data is strictly necessary. Disclosure boundaries are defined in advance, and all third-party contracts include clauses requiring secure handling and deletion of personal data once the purpose is fulfilled.

The company regularly reviews its personal data-sharing arrangements to ensure disclosures remain relevant and necessary. If a vendor relationship ends or the legal basis for disclosure changes, the company halts personal data transfers and verifies that previously shared personal data is securely destroyed. All disclosures are encrypted and logged and employees are trained to understand the limits and conditions under which personal data, such as employee performance metrics or access logs, may be disclosed.

7.3 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Disclosure Principle*:*

	Disclosure Principle Checklist	Y/N
1.	**Predetermination.** Establish the purposes and the legal basis of disclosure before the disclosure of personal data.	
2.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
3.	**Security.** Implement technical security measures to protect personal data (e.g., hashing and encryption) and organisational measures (e.g., policies and contractual obligations) to ensure all personal data is securely handled and disclosed.	
4.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
5.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	
6.	**Third-Party Management**: Ensure that third parties have adequate personal data protection measures in place through contractual agreements or other means before transferring personal data to them.	

PART F: DPbD FOR SECURITY PRINCIPLE

8. Security Principle

Section 9 of Act 709 outlines the Security Principle:

“

(1) A data controller and a data processor shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification,

unauthorized or accidental access or disclosure, alteration or destruction by having regard-

(a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(b) to the place or location where the personal data is stored;

(c) to any security measures incorporated into any equipment in which the personal data is stored;

(d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and

(e) to the measures taken for ensuring the secure transfer of the personal data.

(2) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data processor shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction-

(a) provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and

(b) *take reasonable steps to ensure compliance with those measures*."

8.1 The Security Principle requires that the data controller and data processor take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access disclosure, alteration or destruction.

8.2 The data processor shall guarantee to the data controller that they have sufficiently robust technical and organisational security measures in place to process personal data and subsequently take reasonable steps to comply with that guarantee.

8.3 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Security Principle. They are not prescriptive or exhaustive, and shall be adapted by the data controller and data processor based on the specific risk profile and the personal data processing operations.

(a) **Information security management system:** Implement and maintain operative means of managing policies and procedures for information security.

(b) **Risk analysis:** Assess the risks against the security of personal data by considering the potential impact on the data subject and implementing measures to address identified risks. For risk assessment purposes, develop and maintain a comprehensive, and systematic "threat modelling" and an attack surface analysis of the software design to reduce attack vectors and opportunities to exploit weak points or vulnerabilities.

(c) **Security by design:** Consider security requirements as early as possible in the system design and development, and continuously integrate and perform relevant tests.

(d) **Maintenance:** Regularly review and test software, hardware, systems and services to uncover and address vulnerabilities of the systems supporting the processing of personal data.

(e) **Access control management:** Only authorised personnel who require access to personal data for their processing tasks shall be granted access and such access privileges shall be differentiated based on roles.

(f) **Access limitation:** Data processing shall be designed to ensure that only a minimal number of personnel have access to personal data to perform their duties.

(g) **Access limitation (content):** For each processing operation, limit access only to those attributes per personal data set that are required to perform that operation. Additionally, restrict access to personal data pertaining to only those data subjects who fall within the remit of the respective personnel.

(h) **Access segregation:** Personal data processing shall be designed to ensure that personal data is segregated, such that no authorised individual is required to have comprehensive access to all personal data without a legitimate interest.

(i) **Secure transfers:** Personal data transfers shall be protected against any unauthorised access or unintended changes.

(j) **Secure storage:** Data storage shall be secure from unauthorised access and alterations. Procedures shall be established to assess the risk of centralised or decentralised storage and what categories of personal data this applies to. Certain personal data may require additional security measures or isolation.

(k) **Pseudonymisation:** Personal data shall be pseudonymised as soon as it is no longer necessary for the data to be directly identifiable personal data as a security measure to minimise risks of potential personal data breaches, for example, using hashing or encryption. Identification keys shall be stored separately from the pseudonymised data.

(l) **Backups/logs:** Back-ups and logs shall be maintained to the extent necessary for information security. Audit trails and event monitoring shall be implemented as a routine security control. These records shall be protected from unauthorised or accidental access and alteration.

(m) **Disaster recovery/business continuity:** Information system disaster recovery and business continuity requirements shall be established to ensure timely restoration and the availability of personal data.

(n) **Protection according to risk:** All categories of personal data shall be protected in accordance with the individual risk of each personal data type rather than based solely on the entire data processing risk.

(o) **Security incident response management:** Establish routines, procedures and resources to detect, contain, handle, report and review personal data breaches systematically.

(p) **Incident management:** Establish processes to handle personal data breaches to make the processing system more robust. This includes notification procedures for notifying the Commissioner and affected data subjects.

Example 1:

The café ensure that privacy is embedded in the online ordering system. Customers' personal data are stored and processed in a separate encrypted database system. Before the system launch, a cybersecurity risk assessment is performed on the IT infrastructure to ensure that it functions as expected. Reassessment is performed periodically.

Example 2:

A consulting firm embeds security into its project management and client engagement systems by implementing an information security management system aligned with international standards. Client data, such as financial report, strategic plan and HR record, is stored in encrypted repositories with differentiated access controls based on project roles. During system design, threat modelling is conducted to identify potential vulnerabilities and regular penetration testing ensures ongoing resilience.

Access to personal data is strictly limited to the consultants assigned to specific projects, with further segmentation to restrict access to only relevant personal data attributes. Secure file transfers and encrypted communications are used for client interactions and pseudonymisation is applied when preparing benchmarking or analytical reports. The firm maintains a secure backups and a business continuity plan and has a documented incident response protocol to manage and report a data breach in line with Act 709 obligations.

8.4 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Security Principle*:*

	Security Principle Checklist	Y/N
1.	**Separation.** Establish technological, policy and procedural controls to prevent data linkages (e.g. isolate personal data processed for different purposes in separate databases by default).	
2.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
3.	**Access limitation.** Implement access controls to ensure that access to personal data is granted only to authorised parties with a legitimate need.	
4.	**Security.** Implement security measures to protect personal data throughout its entire lifecycle so that all personal data is collected, processed, transferred, stored and destroyed in a secured manner.	
5.	**Top-level commitment.** Ensure that top management recognises that personal data protection can coexist with legitimate business interests, and establishes a clear commitment to define and enforce high standards of personal data protection.	

Security Principle Checklist		Y/N
6.	**Accountability.** Establish a dedicated function within the organisation (e.g. the Data Protection Officer) responsible for documenting, communicating, overseeing and implementing all personal data protection policies and procedures.	
7.	**Assessment.** Conduct a Data Protection Impact Assessment (DPIA) before the processing to identify personal data risks and implement appropriate mitigation measures.	
8.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	
9.	**Risk assessment and audit.** Conduct regular risk assessments and audits to identify any potential vulnerabilities and compliance gaps.	
10.	**Third party management.** Ensure a third party has adequate personal data protection measures in place through contractual or other means before transferring personal data to that party.	
11.	**Breach management.** Establish adequate procedures and resources to detect, contain, handle, report and learn from personal data breaches.	

PART G: DPbD FOR RETENTION PRINCIPLE

9. Retention Principle

Section 10 of Act 709 outlines the Retention Principle:

"

(1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

(2) *It shall be the duty of a data controller to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed*."

9.1 The Retention Principle requires that the data controller not keep the personal data for longer than is necessary for the fulfilment of purpose for which it was processed.

9.2 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Retention Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Data minimisation:** When further processing personal data, the data controller shall periodically consider whether processed personal data is still adequate,

relevant and necessary, or if it shall be deleted. If the purpose of the processing does not require the final dataset to refer to an identified or identifiable data subject (e.g. for statistical purposes), but the initial processing does (e.g. before data aggregation), then the data controller shall permanently delete personal data as soon as identification is no longer needed.

(b) **Deletion and/ or anonymisation:** Where personal data is not, or is no longer necessary for the purpose, personal data shall be anonymised and/or permanently deleted. There shall be clear internal procedures and functionalities for deletion and/or anonymisation.

(c) **Effectiveness of anonymisation/ deletion:** The data controller shall ensure that it is not possible to re-identify anonymised data or recover deleted data, and shall test whether such re-identification or recovery can be performed.

(d) **Automation:** Deletion of certain personal data shall be automated.

(e) **Retention criteria:** The data controller shall determine what personal data and its length of retention is necessary.

(f) **Justification:** The data controller shall be able to justify why such identified retention period is necessary and be able to disclose the rationale of the retention period, including its legal grounds.

(g) **Enforcement of retention policies:** The data controller shall enforce internal retention policies and conduct tests to ensure they are properly enforced.

(h) **Backups/logs:** The data controller shall determine what personal data and retention periods are necessary for backups and logs.

(i) **Data flow:** The data controller shall be aware of the flow of personal data and the storage of any copies thereof and seek to limit their temporary storage. The personal data flow shall be made efficient enough to not create more copies than necessary.

Example 1:

The database storing customer personal data is designed such that the retention period of each personal data is automatically generated upon its addition to the database and personal data that reaches the expiry of its retention period are automatically deleted.

Example 2:

A local social media platform collects user-generated content[6], location data and behavioural analytics to personalise feeds and serve targeted advertisements. The platform enforces clear personal data retention rules for example, deleting deactivated accounts and associated personal data after a defined period. When a data subject deletes posts or messages, the personal data is securely wiped from both live and backup systems. Personal data shared with advertisers is aggregated

[6] Digital material such as in text, image, video or audio formats created by social media platform users.

and anonymised, ensuring that such the data subject cannot be re-identified, while still enabling business insights.

9.3 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Retention Principle*:*

	Retention Principle Checklist	Y/N
1.	**Data minimisation.** Minimise the collection and processing of personal data to only what is strictly necessary for the identified purpose(s).	
2.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
3.	**Access limitation.** Implement access controls to ensure that access to personal data is granted only to authorised parties with a legitimate need.	
4.	**Security.** Implement security measures to protect personal data throughout its entire lifecycle so that all personal data is collected, processed, transferred, stored and destroyed in a secured manner.	

PART H: DPbD FOR DATA INTEGRITY PRINCIPLE

10. Data Integrity Principle

Section 11 of Act 709 outlines the Data Integrity Principle:

"*A data controller shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed*."

10.1 The Data Integrity Principle requires the data controller to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose for which the personal data was collected and further processed.

10.2 A DPbD approach in compliance with the Data Integrity Principle further requires the data controller to take reasonable steps regarding the personal data of data subjects under the age of eighteen (18) years. This includes ensuring that the sourcing and rectification of such personal data are made easily accessible to the parent, guardian or person who has parental responsibility for that data subject.

10.3 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Data Integrity Principle. They are not prescriptive or

exhaustive and shall be adapted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Data source:** Sources of personal data shall be reliable to ensure personal data accuracy.

(b) **Degree of accuracy**: Each personal data element shall be as accurate as necessary for the specified purposes.

(c) **Attributable recording:** The data controller shall have identifiable records of when and why a personnel or system inserts personal data during the sourcing stage.

(d) **Verification:** Depending on the nature of the personal data, in relation to how often it may change, the data controller shall verify the correctness of personal data with the data subject before and at different stages of the processing (for example, verification requirements depending on attaining retirement age).

(e) **Rectification:** The data controller shall facilitate the rectification of inaccurate data without delay upon the request of the data subject.

(f) **Error-propagation avoidance:** The data controller shall mitigate the effect of accumulated errors in the processing chain.

(g) **Access:** The data subject shall be provided with information and given effective access to personal data in accordance with the Access Principle to ensure accuracy and to rectify as needed.

(h) **Continued accuracy:** Personal data shall be accurate at all stages of the processing and tests as to accuracy shall be carried out at critical steps of processing.

(i) **Up-to-date:** Personal data shall be updated if necessary for the purpose of processing.

(j) **Data design:** The data controller shall use technological and organisational design features to minimise inaccuracy, for example by presenting concise predetermined choices instead of free-text fields.

Example:

A fintech company offers a platform for personal loans. To ensure personal data integrity, the company implements a robust system to verify the accuracy of customer information, as the integrity of this personal data is critical for accurate credit risk assessment and loan disbursement. When a customer applies for a loan, the platform uses a "know your customer" (KYC) verification process that cross-references the personal data provided (name, NRIC number, address) with reliable government and financial databases. This serves as a primary personal data source verification, reducing the risk of errors.

The company also builds features to facilitate user-led data accuracy. During the application process, the platform displays a summary of the provided information, prompting the user to review and confirm its accuracy before submission, thereby providing an opportunity for rectification. For certain dynamic personal data points,

such as an applicant's residential address, the system includes a periodic verification prompt. For instance, six months after a loan is disbursed, the customer receives a notification to confirm if their address or contact details are still up to date, ensuring the personal data remains accurate for ongoing communications and account management.

Furthermore, the company's internal systems are designed to prevent the propagation of errors. Any change to a customer's personal data, whether initiated by the customer or the company's personnel, undergoes an automated validation check before being committed to the central database. This ensures that any inaccuracies are caught at the point of entry and not carried forward into other linked processes, such as credit scoring models or disbursement instructions. This approach safeguards the integrity of the personal data throughout its lifecycle, from collection to processing, thereby protecting both the company from financial risk and the customer from receiving a misleading or inaccurate service.

10.4 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Data Integrity Principle*:*

	Data Integrity Principle	Y/N
1.	**Accessibility.** Put in place mechanisms that enable the data subject to easily access his own personal data.	
2.	**Data design.** Use technological and organisational design features to minimise inaccuracy, for example by presenting concise predetermined choices instead of free-text fields.	
3.	**User Control.** Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	
4.	**Rectification**. Facilitate the rectification of inaccurate personal data without delay upon the request of the data subject.	
5.	**Review.** Conduct regular accuracy tests on personal data.	

PART I: DPbD FOR ACCESS PRINCIPLE

11. Access Principle

Section 12 of Act 709 outlines the Access Principle:

"*A data subject shall be given access to his personal data held by a data controller and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up to date, except where compliance with a request to such access or correction is refused under this Act*."

11.1 The Access Principle requires data controller to allow the data subject to access his personal data and to correct any data that is inaccurate, incomplete, misleading or not up-to-date upon receiving correction requests pursuant to Section 34 of Act 709. The data subject shall be informed of the designated point of contact to whom such requests should be submitted. Contact information shall be easily accessible and located in strategic locations such as within user accounts, in contextual information (e.g., information displayed during the use of services), personal data protection notices (privacy notices), Frequently Asked Questions (FAQs) and other appropriate channels.

11.2 A DPbD approach in compliance with the Access Principle further requires the data controller to design appropriate systems for personal data belonging to the data subject under the age of eighteen (18) years. Such systems shall ensure that access to such personal data is easily accessible to the data subject's parent, guardian or person who has parental responsibility for that data subject.

11.3 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Access Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Clarity:** Information on how to exercise the data subject's right shall be provided in clear, plain, concise and intelligible language.

(b) **Accessibility:** Mechanisms for exercising the data subject's rights shall be easily accessible to the data subject.

(c) **Contextual:** Mechanisms for exercising the data subject's rights shall be provided at the relevant time and in the appropriate form.

(d) **Universal design:** Mechanisms for exercising the data subject's rights shall be accessible to the data subject, including the use of machine-readable languages to facilitate and automate readability and clarity.

(e) **Comprehensible:** The data subject shall have a fair understanding of what he can expect with regards to the extent to which he can exercise his personal data rights.

(f) **Multi-channel:** Mechanisms to exercise the data subject's rights shall be provided through various channels and media, not limited to textual form, to increase the likelihood of the information reaching the data subject effectively.

Example:

The café ensures that customers can easily exercise their rights regarding their personal data. Within their respective account profiles, quick access options are available for customers to download their personal data in an accessible format, update their data or delete accounts. Customers will be notified immediately upon receipt of their request and provided with instructions on how to track their request status until the verification stage. In addition, contact details are provided should customers require further support.

11.4 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Access Principle:

	Access Principle Checklist	Y/N
1.	**Accessibility.** Provide mechanisms that enable the data subject to easily access his own personal data.	
2.	**User-centred design.** Design systems that respect the data subject's interests through strong privacy defaults and personal data protection notices (privacy notices) that are easily accessible and located in appropriate places.	
3.	**User Control.** Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	

12. Checklist

12.1 A checklist has been developed to guide the implementation of the DPbD approach. The checklist as provided in **Annex A**, outlines non-exhaustive measures for implementing DPbD, organised into two (2) categories:

(a) **Data-Oriented Measures:** focusing on the technical aspects of data processing; and

(b) **Process-Oriented Measures:** focusing on the organisational and procedural aspects of data processing.

PART J: BEST PRACTICES FOR DPbD GOVERNANCE

13. Best practices

13.1 DPbD is about establishing an organisational culture that adopts a principled, proactive approach to personal data management. This approach shall be applied across the organisation and reflected in its products, services, governance and operations. This shall involve:

(a) a clear commitment from senior management to set and enforce high standards of data protection;

(b) fostering a culture where all stakeholders share a commitment to continuous improvement in data protection standards; and

(c) establishing processes to identify gaps in current designs and practices and address issues before they occur proactively and systematically.

13.2 The following illustration outlines best practices for implementing DPbD governance. These are non-mandatory and intended to guide organisations, which are encouraged

to apply them using a risk-based approach aligned with their respective risk profile and operational context.

(a) Ensuring senior leadership commitment and their active participation in establishing a robust and proactive personal data protection framework, such as by:

  (i) ensuring the Board of Directors includes members with data protection expertise or ensuring directors receive adequate training in the field;

  (ii) ensuring directors allocate sufficient resources to DPbD measures, including for technological enhancements;

  (iii) designating at least one senior manager or Head of Department to be responsible for the organisation's personal data compliance;

  (iv) incorporating personal data protection compliance into senior management performance evaluation;

  (v) mandating regular personal data assessments and audits to be reported to the Board of Directors;

  (vi) hold regular meetings with the organisation's Data Protection Officer (DPO), where applicable.

(b) Conducting periodic audits of personal data protection policies to verify their practical effectiveness and operational compliance.

(c) Developing systematic methods, including Data Protection Impact Assessments (DPIA) to identify and assess risks to ensure any negative impacts are mitigated before they occur.

(d) Fostering a culture and environment where all stakeholders including users, are encouraged to suggest improvements to data protection practices, and ensuring such suggestions are systematically reviewed and adopted where appropriate.

ANNEX A: DATA-ORIENTED AND PROCESS-ORIENTED MEASURES CHECKLIST

Data-Oriented Measures		Y/N
1.	**Predetermination.** Establish the purposes and the legal basis for processing before the processing takes place.	
2.	**Specificity.** Define the purpose(s) for processing as narrowly and specifically as possible.	
3.	**Data minimisation.** Minimise the collection and processing of personal data to only what is strictly necessary for the identified purpose(s).	
4.	**Separation.** Establish technological, policy and procedural controls to prevent combining personal data sets obtained from different sources, commonly referred to as data linkages. For example, isolate personal data processed for different purposes in separate databases by default.	
5.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
6.	**Access limitation.** Implement access controls to ensure that access to personal data is granted only to authorised parties with a legitimate need.	
7.	**Security.** Implement security measures to protect personal data throughout its entire lifecycle so that all personal data is collected, processed, transferred, stored and destroyed in a secured manner.	
8.	**User-centred design.** Design systems that respect the data subject's interests through strong privacy defaults and personal data protection notices (privacy notices) that are easily accessible and located in appropriate places.	
Process-Oriented Measures		
9.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
10.	**Notice.** Provide a personal data protection notice (privacy notice) in both the National Language and English, using clear and plain language and ensure that the notice is easily accessible and, where applicable, communicated through multiple channels or media.	
11.	**User Control.** Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	
12.	**Top-level commitment.** Ensure that top management recognises that personal data protection can coexist with legitimate business interests, and	

	establishes a clear commitment to define and enforce high standards of personal data protection.	
13.	**Accountability.** Establish a dedicated function within the organisation (e.g. the Data Protection Officer) responsible for documenting, communicating, overseeing and implementing all personal data protection policies and procedures.	
14.	**Assessment.** Conduct a Data Protection Impact Assessment (DPIA) before the processing to identify personal data risks and implement appropriate mitigation measures.	
15.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	
16.	**Risk assessment and audit.** Conduct regular risk assessments and audits to identify any potential vulnerabilities and compliance gaps.	
17.	**Third-Party Management**: Ensure that third parties have adequate personal data protection measures in place through contractual agreements or other means before transferring personal data to such parties.	
18.	**Breach management.** Establish adequate procedures and resources to detect, contain, handle, report and learn from personal data breaches.	