TATAAMALAN UMUM PERLINDUNGAN DATA PERIBADI

DIKELUARKAN OLEH

Pejabat Pesuruhjaya Perlindungan Data Peribadi

TARIKH KUATKUASA

15 Disember 2022

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

No. Ruj.
CoP_Umum

PADA menjalankan kuasa yang diberikan oleh Seksyen 24(1) Akta Perlindungan Data Peribadi 2010 [*Akta 709*], saya dengan ini mendaftarkan Tataamalan Umum bagi Golongan Pengguna Data dan terpakai kepada semua pengguna data di bawah Golongan tersebut berkuatkuasa serta-merta.

Bertarikh pada: 15 Disember 2022

(MAZMALEK BIN MOHAMAD)
Pesuruhjaya Perlindungan Data Peribadi, Malaysia

PRAKATA

Tataamalan Umum Perlindungan Data Peribadi ini bertujuan untuk menguatkuasakan pematuhan kepada Seksyen 23 Akta Perlindungan Data Peribadi 2010 [*Akta 709*], peraturan-peraturan dan standard serta mewujudkan garis panduan kepada Golongan Pengguna Data yang tidak menyediakan Tataamalan dan tidak ada forum pengguna data untuk membangunkan Tataamalan yang berkaitan. Sekiranya memerlukan maklumat lanjut, sila rujuk —

Pesuruhjaya Perlindungan Data Peribadi di —
Aras 6, Kompleks KKD, Lot 4G9
Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya, Malaysia
Tel: 03-8000 8000 | Faks: 03-8911 7959
E-mel: info@pdp.gov.my

FOREWORD

This General Code of Practice of Personal Data Protection aims to enforce compliance to Section 23 of the Personal Data Protection Act [*Act 709*], regulations and standard and establish a guideline to the Class of Data Users who have not prepared a Code of Practice and there is no data user forum to develop the relevant Code of Practice for the Class of Data Users. Should you require further information, kindly consult —

The Personal Data Protection Commissioner at —
6th Floor, KKD Complex, Lot 4G9
Persiaran Perdana, Precint 4
Federal Government Administrative Centre
62100 Putrajaya Federal Territory
Malaysia
Tel: 03-89115000 Fax: 03-8911 7959
E-mail: info@pdp.gov.my

ISI KANDUNGAN

1. PENGENALAN

1.1 Latar Belakang

1.1.1 Menurut Penetapan Tarikh Permulaan Kuat Kuasa [*P.U. (B) 464/2013*], Akta Perlindungan Data Peribadi 2010 [*Akta 709*] mula berkuat kuasa pada 15 November 2013. Di bawah Akta 709, sesuatu badan yang dinamakan oleh Pesuruhjaya Perlindungan Data Peribadi sebagai suatu forum pengguna data berkenaan dengan sesuatu Golongan Pengguna Data yang khusus boleh menyediakan suatu Tataamalan.

1.1.2 Seksyen 24 Akta 709 menyediakan keadaan-keadaan di mana Pesuruhjaya Perlindungan Data Peribadi boleh mengeluarkan Tataamalan. Tataamalan Umum Perlindungan Data Peribadi ini hendaklah terpakai kepada Golongan Pengguna Data yang tidak menyediakan suatu Tataamalan dan tidak ada forum pengguna data untuk membangunkan Tataamalan yang berkaitan bagi Golongan Pengguna Data.

1.1.3 Objektif Tataamalan Umum Perlindungan Data Peribadi ini adalah untuk menetapkan amalan-amalan terbaik kepada pengguna data bagi membantu pengguna data dalam memenuhi keperluan di bawah Akta 709 semasa menjalankan transaksi komersial. Contoh-contoh yang disediakan dalam Tataamalan Umum Perlindungan Data Peribadi ini bukanlah secara menyeluruh tetapi adalah untuk tujuan ilustrasi. Cadangan-cadangan yang disediakan dalam Tataamalan Umum Perlindungan Data Peribadi ini adalah amalan-amalan yang baik dan pengguna data digalakkan untuk menerima pakai amalan-amalan ini.

1.1.4 Tataamalan Umum Perlindungan Data Peribadi ini hendaklah dibaca bersama dengan Akta 709, peraturan-peraturan, tindakan-tindakan, perintah-perintah, arahan-arahan, pemberitahuan-pemberitahuan, kelulusan-kelulusan, keputusan-keputusan dan tindakan-tindakan pentadbiran lain dengan apa cara sekalipun disebut, dibuat, diberikan atau dilakukan oleh Pesuruhjaya Perlindungan Data Peribadi.

1.2 **Ketidakpatuhan Tataamalan Umum Perlindungan Data Peribadi**

1.2.1 Tataamalan Umum Perlindungan Data Peribadi ini mempunyai kuasa undang-undang dan berkuat kuasa sebaik sahaja didaftarkan oleh Pesuruhjaya Perlindungan Data Peribadi. Memandangkan Tataamalan Umum Perlindungan Data Peribadi ini terikat secara sah, mana-mana pengguna data yang tidak mematuhi mana-mana peruntukan Tataamalan Umum Perlindungan Data Peribadi ini yang terpakai bagi pengguna data itu melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi satu tahun atau kedua-duanya di bawah Seksyen 29 Akta 709.

2. TAFSIRAN

Bagi tujuan Tataamalan Umum Perlindungan Data Peribadi ini, pelbagai perkataan dan istilah yang digunakan dalam Tataamalan Umum Perlindungan Data Peribadi ini hendaklah mempunyai maksud yang sama seperti dalam Akta 709, kecuali dinyatakan sebaliknya.

Perkataan	Maksud
data peribadi	apa-apa maklumat yang berkenaan dengan transaksi komersial yang — (a) sedang diproses secara keseluruhannya atau sebahagiannya melalui kelengkapan yang dikendalikan secara automatik sebagai tindak balas kepada arahan yang diberikan bagi maksud itu; (b) direkodkan dengan niat bahawa ia sepatutnya diproses secara keseluruhannya atau sebahagiannya melalui kelengkapan itu; atau (c) direkodkan sebagai sebahagian daripada sistem pemfailan yang berkaitan atau dengan niat bahawa ia sepatutnya menjadi sebahagian daripada sistem pemfailan yang berkaitan, yang berhubungan secara langsung atau tidak langsung dengan seorang subjek data, yang dikenal pasti

	atau boleh dikenal pasti daripada maklumat itu atau daripada maklumat lain dalam milikan seseorang pengguna data, termasuk apa-apa data peribadi sensitif dan pernyataan pendapat tentang subjek data itu; tetapi tidak termasuk apa-apa maklumat yang diproses bagi maksud sesuatu perniagaan pelaporan kredit yang dijalankan oleh sesuatu agensi pelaporan kredit di bawah Akta Agensi Pelaporan Kredit 2010
data peribadi sensitif	apa-apa data peribadi yang mengandungi maklumat tentang kesihatan atau keadaan fizikal atau mental seorang subjek data, pendapat politiknya, kepercayaan agamanya atau kepercayaan lain yang bersifat seumpamanya, pelakuan atau pengataan pelakuan apa-apa kesalahan olehnya atau apa-apa data peribadi lain yang ditentukan oleh Menteri melalui perintah yang disiarkan dalam *Warta*
kepentingan vital	perkara yang berhubungan dengan kehidupan, kematian atau keselamatan seorang subjek data
menggunakan	berhubung dengan data peribadi, tidak termasuk perbuatan mengumpul atau menzahirkan data peribadi itu
mengumpul	berhubung dengan data peribadi, ertinya perbuatan yang melaluinya data peribadi itu termasuk ke dalam atau berada di bawah kawalan seorang pengguna data
Menteri	ertinya Menteri yang dipertanggungkan dengan tanggungjawab bagi perlindungan data peribadi
menzahirkan	berhubung dengan data peribadi, ertinya perbuatan yang melaluinya data peribadi itu disediakan oleh seorang pengguna data
orang yang berkaitan	berhubung dengan seorang subjek data, dengan apa jua cara sekalipun diperihalkan, ertinya — (a) dalam hal seorang subjek data yang di bawah umur lapan belas tahun, ibu bapa penjaga atau seseorang yang mempunyai tanggungjawab ibu bapa terhadap subjek data itu;

	(b) dalam hal seorang subjek data yang tidak berupaya menguruskan hal-ehwalnya sendiri, seorang yang dilantik oleh mahkamah untuk menguruskan hal-ehwal itu, atau seorang yang diberi kuasa secara bertulis oleh subjek data untuk bertindak bagi pihak subjek data; atau (c) dalam mana-mana hal lain, seorang yang diberi kuasa secara bertulis oleh subjek data untuk membuat suatu permintaan mengakses data, permintaan pembetulan data, atau kedua-dua permintaan itu, bagi pihak subjek data itu
pemasaran langsung	ertinya berkomunikasi dengan apa cara sekalipun mengenai apa-apa bahan pengiklanan atau pemasaran yang ditujukan kepada individu tertentu
pembetulan	berhubung dengan data peribadi, termasuk pindaan, perubahan, ubah suaian atau pemotongan
peminta	berhubung dengan suatu permintaan mengakses data atau permintaan pembetulan data, ertinya subjek data atau orang yang berkaitan bagi pihak subjek data itu, yang membuat permintaan itu
pemproses data	berhubung dengan data peribadi, ertinya mana-mana orang, selain seorang pekerja pengguna data, yang memproses data peribadi itu semata-mata bagi pihak pengguna data itu, dan tidak memproses data peribadi itu bagi apa-apa maksud persendiriannya
pemprosesan	berhubung dengan data peribadi, ertinya mengumpul, merekod, memegang atau menyimpan data peribadi itu atau menjalankan apa-apa pengendalian atau set pengendalian terhadap data peribadi itu, termasuk — (a) penyusunan, penyesuaian atau pengubahan data peribadi; (b) mendapatkan kembali, merujuk kepada atau menggunakan data peribadi; (c) penzahiran data peribadi melalui penghantaran, pemindahan, penyebaran atau selainnya menjadikannya tersedia; atau

	(d) penjajaran, penggabungan, pembetulan, pemadaman atau pemusnahan data peribadi
pengguna data	ertinya seseorang yang sama ada berseorangan atau bersesama atau bersama dengan orang lain memproses apa-apa data peribadi atau mempunyai kawalan terhadap atau membenarkan pemprosesan apa-apa data peribadi, tetapi tidak termasuk seorang pemproses data
pengguna data yang berkaitan	berhubung dengan — (a) sesuatu pemeriksaan, ertinya pengguna data yang menggunakan sistem data peribadi yang menjadi subjek pemeriksaan itu; (b) sesuatu aduan, ertinya pengguna data yang dinyatakan dalam aduan itu; (c) sesuatu penyiasatan — (i) dalam hal suatu penyiasatan yang dimulakan dengan sesuatu aduan, ertinya pengguna data yang dinyatakan dalam aduan itu; (ii) dalam mana-mana hal lain, ertinya pengguna data yang menjadi subjek penyiasatan itu; (d) sesuatu notis penguatkuasaan, ertinya pengguna data yang menjadi subjek penyiasatan itu
pihak ketiga	berhubung dengan data peribadi, ertinya mana-mana orang selain — (a) seorang subjek data; (b) seorang yang berkaitan yang berhubungan dengan seorang subjek data; (c) seorang pengguna data; (d) seorang pemproses data; atau (e) seorang yang diberi kuasa secara bertulis oleh pengguna data untuk memproses data peribadi di bawah kawalan langsung pengguna data itu
standard	ertinya suatu kehendak minimum yang dikeluarkan oleh Pesuruhjaya Perlindungan Data Peribadi, yang

	memperuntukkan, bagi kegunaan biasa dan berulang, kaedah-kaedah, garis panduan atau ciri-ciri bagi aktiviti atau keputusan aktiviti itu, yang matlamatnya adalah pencapaian peringkat susunan yang optimum dalam sesuatu konteks yang diberikan
subjek data	ertinya seseorang individu yang menjadi subjek data peribadi itu
transaksi komersial	ertinya apa-apa transaksi bersifat komersial, sama ada secara kontrak atau tidak, yang termasuk apa-apa perkara yang berhubungan dengan pembekalan atau pertukaran barang atau perkhidmatan, agensi, pelaburan, pembiayaan, perbankan dan insurans, tetapi tidak termasuk sesuatu perniagaan pelaporan kredit yang dijalankan oleh sesuatu agensi pelaporan kredit di bawah Akta Agensi Pelaporan Kredit 2010

3. PRINSIP AM (SEKSYEN 6 AKTA 709)

3.1 Prinsip Am menyediakan —

(a) pengguna data adalah dikehendaki untuk mendapatkan persetujuan daripada subjek data sebelum memproses data peribadi kecuali pemprosesan data peribadi itu melibatkan salah satu daripada keadaan-keadaan berikut:

(i) bagi melaksanakan sesuatu kontrak yang subjek data itu ialah satu pihak kepadanya;

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

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

(iv) bagi melindungi kepentingan vital subjek data itu;

(v) bagi mentadbirkan keadilan; atau

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

(b) bagi pemprosesan data peribadi sensitif, pengguna data adalah dikehendaki untuk memperoleh persetujuan subjek data secara nyata.

3.2 Pemprosesan data peribadi yang merangkumi data peribadi sensitif hanya boleh dilakukan sekiranya —

(a) data subjek telah memberikan persetujuannya;

(b) data peribadi diproses bagi tujuan yang sah;

(c) pemprosesan data peribadi adalah perlu atau berkaitan secara langsung dengan tujuan ianya diproses; dan

(d) data peribadi yang diperoleh adalah mencukupi, relevan dan tidak berlebihan bagi tujuan data peribadi itu diproses.

3.3 **Persetujuan subjek data**

3.3.1 Pengguna data hendaklah memperoleh persetujuan daripada subjek data berhubung dengan pemprosesan data peribadi dalam apa-apa bentuk yang persetujuan itu boleh direkodkan dan disenggarakan dengan sewajarnya oleh pengguna data itu.[1] Sekiranya bentuk persetujuan yang diberikan melibatkan juga perkara lain, kehendak untuk memperoleh persetujuan hendaklah dikemukakan secara berbeza dalam pengemukaannya daripada perkara lain itu.

3.3.2 Persetujuan bagi mengumpul, memproses dan menzahirkan data peribadi subjek data boleh diperoleh dalam pelbagai cara. Persetujuan itu menyediakan indikasi yang jelas bahawa subjek data telah memberikan persetujuannya terhadap tujuan pengumpulan, pemprosesan atau penzahiran data peribadinya sebagaimana yang telah dimaklumkan.

[1] Subperaturan 3(1) Peraturan-peraturan Perlindungan Data Peribadi 2013 [*P.U. (A) 335/2013*]

3.3.3 Contoh bentuk-bentuk persetujuan —

(a) tandatangan atau petak yang boleh diklik untuk menunjukkan persetujuan

☐ Saya dengan ini membenarkan pemprosesan data peribadi yang telah saya berikan dalam borang ini untuk tujuan _____ sahaja. (nyatakan tujuan) Nama: Nombor kad pengenalan: ***Contoh:*** *Dengan mengklik butang "Setuju" melalui permohonan dalam talian, ia menunjukkan bahawa subjek data telah memberikan persetujuan untuk pemprosesan data peribadi.*

(b) persetujuan melalui perlakuan atau perbuatan: persetujuan adalah dianggap sebagai telah diberikan dengan cara perlakuan atau perbuatan jika —

(i) subjek data tidak membantah pemprosesan itu;

(ii) subjek data menzahirkan data peribadinya secara sukarela; atau

(iii) subjek data terus menggunakan perkhidmatan pengguna data; dan

Contoh: *Persetujuan diberikan oleh subjek data apabila memberikan suatu salinan dokumen pengenalan diri kepada pengguna data, sama ada ia mengandungi data peribadi sensitif atau tidak.*

(c) persetujuan lisan: hendaklah direkodkan secara digital (seperti melalui penggunaan rekod panggilan dan/atau perisian perakam panggilan) atau dengan mengeluarkan pemakluman (seperti mengeluarkan surat, borang atau e-mel daripada e-mel rasmi

pengguna data) kepada subjek data yang mengesahkan bahawa persetujuan telah diberikan.

Contoh: *Persetujuan diberikan oleh seorang pemanggil kepada pengguna data untuk memproses data peribadi pemanggil apabila pemanggil menghubungi khidmat pelanggan pengguna data untuk perkhidmatan mereka.*

3.3.4 Pengguna data hendaklah mendapatkan persetujuan daripada ibu bapa, penjaga atau seseorang yang mempunyai tanggungjawab ibu bapa terhadap subjek data, sekiranya subjek data itu berumur bawah lapan belas (18) tahun.

3.3.5 Pengguna data hendaklah mendapatkan persetujuan daripada seseorang yang dilantik oleh mahkamah untuk menguruskan hal ehwal subjek data atau seseorang yang diberikan kuasa secara bertulis oleh subjek data untuk bertindak bagi pihaknya sekiranya subjek data itu tidak berupaya untuk menguruskan hal ehwalnya sendiri.

4. PRINSIP NOTIS DAN PILIHAN (SEKSYEN 7 AKTA 709)

4.1 Pengguna data adalah dikehendaki untuk menyediakan notis bertulis, yang juga dikenali sebagai Notis Perlindungan Data Peribadi (PDP), kepada subjek data sebelum atau dengan kadar segera selepas pengumpulan data peribadinya. Notis PDP adalah pemakluman bertulis kepada subjek data mengenai pengendalian data peribadinya.

4.2 Dengan meneliti Notis PDP, subjek data seharusnya mendapat gambaran jelas mengenai bagaimana pengguna data akan memproses data peribadinya yang telah dikemukakan dan pilihan-pilihan yang ada kepada subjek data. Notis PDP tidak seharusnya menjadi platform bagi pengguna data untuk mendapatkan persetujuan subjek data, terutama suatu persetujuan yang menyeluruh. Pengguna data hendaklah memperoleh persetujuan itu dengan cara yang sepatutnya, merekod dan mengendalikannya dengan munasabah.

4.3 Bilakah Notis PDP perlu dikemukakan

4.3.1 Notis PDP hendaklah diberikan dengan secepat yang dapat dilaksanakan oleh pengguna data —

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

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

(c) sebelum pengguna data itu menggunakan data peribadi subjek data itu bagi maksud selain maksud yang baginya data peribadi itu dikumpulkan; atau

(d) sebelum pengguna data itu menzahirkan data peribadi itu kepada pihak ketiga.

4.4 Elemen-elemen Wajib

4.4.1 Notis PDP hendaklah mengandungi elemen-elemen wajib seperti yang berikut:

(a) data peribadi yang diproses
- untuk menamakan butiran data peribadi yang terlibat
- jenis data peribadi – untuk menyatakan sebarang data peribadi sensitif yang terlibat dalam pemprosesan
- untuk menyatakan sama ada data peribadi kanak-kanak di bawah umur lapan belas (18) tahun adalah diproses

(b) keperluan untuk memproses
- tujuan pemprosesan
- untuk menyatakan sama ada terdapat keperluan badan kawal selia untuk mengumpul data peribadi tertentu
- berapa lamakah data peribadi akan disimpan untuk

pemprosesan itu

- bilakah data peribadi akan dilupuskan
- apakah langkah-langkah praktikal yang akan diambil untuk memastikan data peribadi adalah selamat

(c) sumber data peribadi

- untuk menyatakan semua sumber dalaman dan luaran yang merujuk kepada dari mana data peribadi diperolehi (contoh: aplikasi/borang pendaftaran manual atau digital)

(d) hak-hak subjek data

- pilihan data peribadi yang dikemukakan – wajib atau satu pilihan. Sekiranya data peribadi itu adalah wajib, nyatakan kesan-kesan sekiranya ianya tidak dikemukakan
- bagaimana untuk mengakses data peribadi yang telah dikemukakan kepada pengguna data
- bagaimana untuk membetulkan atau mengemas kini data peribadi
- bagaimana untuk mengehadkan pemprosesan data peribadi yang dikemukakan – bagaimana untuk menarik balik persetujuan untuk memproses data peribadi
- bagaimana untuk menghubungi pengguna data bagi mengemukakan pertanyaan atau aduan berkaitan data peribadi – untuk menyatakan nama pegawai bertanggungjawab, jawatan, nombor telefon dan alamat e-mel untuk dihubungi

(e) penzahiran data peribadi

- untuk menamakan pihak ketiga yang terlibat dengan penzahiran dan keperluan penzahiran itu
- untuk memaklumkan langkah-langkah keselamatan yang diambil untuk memastikan penzahiran yang dilaksanakan adalah selamat dan terjamin

4.4.2 Bagi maksud perenggan 7(1)*(d)* Akta 709, pengguna data hendaklah sekurang-kurangnya memberikan subjek data perincian seperti yang berikut:

(a) perjawatan orang yang boleh dihubungi;

(b) nombor telefon;

(c) nombor faks, sekiranya ada;

(d) alamat e-mel, sekiranya ada; dan

(e) apa-apa maklumat lain yang berkaitan.[2]

4.5 **Bahasa**

4.5.1 Notis PDP hendaklah dalam dwibahasa; bahasa kebangsaan dan bahasa Inggeris. Sekiranya terdapat keperluan untuk menyediakan Notis PDP dalam bahasa-bahasa lain, pengguna data boleh berbuat demikian.

4.6 **Kaedah Penyampaian**

4.6.1 Pengguna data boleh menyampaikan Notis PDP kepada subjek data melalui satu atau lebih kaedah-kaedah berikut:

(a) menghantar salinan bercetak Notis PDP ke alamat akhir subjek data yang diketahui berdasarkan rekod pengguna data;

(b) memaparkan Notis PDP di laman web pengguna data;

(c) dengan menghantar khidmat pesanan ringkas (SMS) berserta alamat laman web/pautan kepada Notis PDP dan/atau nombor telefon kepada subjek data bagi tujuan meminta Notis PDP dan/atau maklumat lanjut;

[2] Peraturan 4 Peraturan-peraturan Perlindungan Data Peribadi 2013 [*P.U. (A) 335/2013*]

(d) menghantar e-mel berserta alamat laman web/pautan ke Notis PDP pengguna data dan/atau nombor telefon kepada subjek data untuk dihubungi bagi mendapatkan maklumat lanjut;

(e) menghantar mesej elektronik berserta alamat laman web/pautan ke Notis PDP pengguna data dan/atau nombor telefon kepada subjek data untuk dihubungi bagi mendapatkan maklumat lanjut melalui saluran elektronik yang digunakan oleh pengguna data;

(f) menyertakan ringkasan Notis PDP ke dalam yang merupakan amalan komunikasi lazim dengan subjek data (sebagai contoh, penyata bil bulanan) berserta alamat laman web/pautan ke Notis PDP dan/atau nombor telefon untuk dihubungi bagi mendapatkan Notis PDP dan/atau maklumat lanjut;

(g) memaparkan secara jelas ringkasan Notis PDP di premis perniagaan pengguna data (sebagai contoh, di meja kaunter yang dilawati subjek data dan/atau di lokasi utama premis pengguna data), dan menyediakan Notis PDP yang lengkap apabila diminta di kaunter atau kepada pekerja pengguna data;

(h) memaparkan pemakluman pada kios-kios berserta alamat laman web/pautan ke Notis PDP, nombor telefon untuk dihubungi bagi mendapatkan maklumat lanjut dan/atau menyatakan bahawa Notis PDP tersebut di cawangan pengguna data;

(i) memasukkan pernyataan dalam mana-mana borang permohonan/pendaftaran yang merujuk kepada Notis PDP, yang boleh diakses melalui alamat laman web/pautan yang diberi, atau dengan membuat permintaan kepada pekerja pengguna data, atau dengan menghubungi nombor telefon yang tertera di borang permohonan/pendaftaran;

(j) mencetak salinan Notis PDP dan menyerahkannya kepada

subjek data di premis pengguna data; atau

(k) sebarang kaedah komunikasi lain yang dapat digunakan bagi menyampaikan Notis PDP kepada subjek data.

4.6.2 Pengguna data hendaklah menentukan kaedah yang paling sesuai untuk mengkomunikasi Notis PDP yang boleh sampai kepada seberapa banyak subjek data. Adalah disyorkan supaya pengguna data menggunakan pelbagai kaedah komunikasi untuk memastikan bahawa Notis PDP dikomunikasikan secara meluas.

4.6.3 Pengguna data adalah dikehendaki untuk menyimpan rekod setelah menyampaikan Notis PDP kepada subjek data. Keperluan ini adalah untuk mengekalkan bukti atau rekod bahawa pengguna data telah mengkomunikasikan Notis PDP kepada subjek data.

4.6.4 Pengguna data boleh merujuk kepada sampel templat Notis PDP yang dikeluarkan oleh Pesuruhjaya Perlindungan Data Peribadi yang dilampirkan sebagai **Lampiran 1**.

5. PRINSIP PENZAHIRAN (SEKSYEN 8 AKTA 709)

5.1 Penzahiran data peribadi milik subjek data terhad kepada tujuan dan tujuan yang berkaitan yang telah memperolehi persetujuan asal di bawah Prinsip Notis dan Pilihan. Tujuan pengisytiharan oleh pengguna data dalam Notis PDP untuk pengumpulan data peribadi adalah penting kerana ia mempengaruhi sama ada persetujuan tambahan perlu diperolehi di bawah Prinsip Penzahiran. Prinsip Penzahiran berkait rapat dengan Prinsip Notis dan Pilihan.

5.2 Tiada data peribadi boleh, tanpa persetujuan subjek data, dizahirkan bagi apa-apa maksud selain —

(a) maksud yang baginya data peribadi itu hendak dizahirkan pada masa pengumpulan data peribadi itu;

(b) suatu maksud yang berhubungan secara langsung dengan maksud asal; atau

(c) kepada mana-mana pihak selain pihak ketiga daripada golongan pihak ketiga yang dinyatakan dalam Notis PDP.

5.3 Had penzahiran data peribadi boleh dilanjutkan di luar persetujuan yang telah diberikan oleh subjek data untuk tujuan asal semasa pengumpulan. Penzahiran itu boleh dilakukan dalam keadaan seperti yang berikut:[3]

(a) subjek data itu telah memberikan persetujuannya bagi penzahiran itu;

(b) penzahiran itu —
  (i) perlu bagi maksud mencegah atau mengesan suatu jenayah, atau bagi maksud penyiasatan; atau
  (ii) dikehendaki atau dibenarkan oleh atau di bawah mana-mana undang-undang atau oleh perintah suatu mahkamah;

(c) pengguna data bertindak atas kepercayaan yang munasabah bahawa dia ada hak di sisi undang-undang untuk menzahirkan data peribadi itu kepada orang lain itu;

(d) pengguna data bertindak atas kepercayaan yang munasabah bahawa dia akan mendapat persetujuan subjek data jika subjek data itu mengetahui tentang penzahiran data peribadi itu dan hal keadaan mengenai penzahiran itu; atau

(e) penzahiran itu berjustifikasi oleh sebab ia berkepentingan awam dalam hal keadaan yang ditentukan oleh Menteri.

[3] Seksyen 39 Akta 709

5.4 **Senarai penzahiran**

5.4.1 Pengguna data hendaklah menyimpan dan menyenggara suatu senarai penzahiran kepada pihak ketiga bagi maksud perenggan 8*(b)* Akta 709 berhubung dengan data peribadi subjek data yang telah atau sedang diproses olehnya.[4]

5.5 **Penzahiran kepada pemproses data**

5.5.1 Pengguna data berkemungkinan besar menzahirkan data peribadi kepada pemproses data untuk pelbagai tujuan berkenaan dengan perniagaan pengguna data. Di mana pemproses data terlibat, adalah disyorkan supaya pengguna data memperoleh jaminan daripada pemproses data berkenaan dengan data peribadi yang akan dizahirkan. Jaminan-jaminan ini boleh termasuk, antara lain —

(a) pemproses data hanya akan memproses data peribadi untuk tujuan yang berkaitan dengan lantikan oleh pengguna data, selaras dengan arahan pengguna data, dan tiada tujuan lain; dan

(b) pemproses data akan mematuhi semua undang-undang, pengawalseliaan dan standard industri berkaitan dengan privasi, kerahsiaan atau keselamatan data peribadi.

6. PRINSIP KESELAMATAN (SEKSYEN 9 AKTA 709)

6.1 Pengguna data hendaklah, apabila memproses data peribadi, mengambil langkah yang praktikal untuk melindungi data peribadi itu daripada apa-apa kehilangan, salah guna, ubahsuaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan dengan mengambil kira —

[4] Peraturan 5 Peraturan-peraturan Perlindungan Data Peribadi 2013 [*P.U. (A) 335/2013*]

(a) sifat data peribadi itu dan kemudaratan akibat daripada kehilangan, salah guna, ubahsuaian, 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.[5]

6.2 Maksud langkah praktikal akan berbeza daripada satu kes kepada kes yang lain, bergantung kepada sifat data peribadi yang diproses oleh pengguna data dan tahap kepekaan yang berhubung kait kepada data peribadi atau membahayakan di mana subjek data mungkin mengalami kehilangan, penyalahgunaan, pengubahsuaian, akses atau penzahiran, pemindahan atau pemusnahan tanpa kebenaran atau tidak sengaja.

6.3 **Penetapan standard keselamatan bagi data peribadi yang diproses secara elektronik**

6.3.1 Pengguna data hendaklah menyediakan langkah-langkah keselamatan yang praktikal ketika pemprosesan data peribadi untuk melindungi data peribadi itu daripada apa-apa kehilangan, salah guna, ubahsuaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan dengan mengambil kira faktor berikut:[6]

[5] Subseksyen 9(1) Akta 709
[6] Bahagian II, No. 4, Standard Perlindungan Data Peribadi 2015

KESELAMATAN DATA PERIBADI SECARA ELEKTRONIK	
Bil.	**Perkara**
1.	Mendaftarkan semua kakitangan yang terlibat dalam pemprosesan data peribadi.
2.	Menamatkan hak akses kakitangan kepada sistem data peribadi selepas kakitangan berhenti kerja, diberhentikan kerja, ditamatkan kontrak atau perjanjian, atau diselaraskan mengikut perubahan dalam organisasi.
3.	Mengawal dan mengehadkan takat kuasa kakitangan untuk mengakses data peribadi bagi tujuan mengumpul, memproses dan menyimpan data peribadi.
4.	Menyediakan ID pengguna dan kata laluan untuk kakitangan yang diberi kebenaran mengakses data peribadi.
5.	Membatalkan ID pengguna dan kata laluan dengan serta-merta apabila kakitangan yang diberi kebenaran mengakses data peribadi tidak lagi mengendalikan data peribadi.
6.	Menetapkan prosedur keselamatan fizikal seperti yang berikut: i. mengawal pergerakan keluar dan masuk ke tempat penyimpanan data; ii. menyimpan data peribadi di lokasi yang bersesuaian iaitu selamat daripada ancaman fizikal atau semula jadi serta tidak terdedah; iii. menyediakan kamera litar tertutup di tempat penyimpanan data (sekiranya perlu); dan iv. menyediakan kawalan keselamatan dua puluh empat (24) jam sehari (sekiranya perlu).
7.	Mengemas kini *Back Up/Recovery System* dan perisian anti-virus bagi melindungi data peribadi daripada insiden pencerobohan dan sebagainya.
8.	Melindungi sistem komputer daripada ancaman *malware* bagi mengelakkan serangan ke atas data peribadi.
9.	Pemindahan data peribadi melalui peranti media mudah alih (*removable media device*) dan perkhidmatan pengkomputeran awan (*cloud computing service*) adalah tidak dibenarkan kecuali dengan kebenaran bertulis

	pegawai yang diberi kuasa oleh pengurusan tertinggi organisasi pengguna data.
10.	Merekodkan sebarang pemindahan data peribadi yang menggunakan peranti media mudah alih (*removable media device*) dan perkhidmatan pengkomputeran awan (*cloud computing service*).
11.	Pemindahan data peribadi melalui perkhidmatan pengkomputeran awan (*cloud computing service*) perlu mematuhi prinsip-prinsip perlindungan data peribadi di Malaysia dan negara-negara lain yang mempunyai undang-undang perlindungan data peribadi.
12.	Menyelenggara rekod akses ke atas data peribadi secara berkala dengan sempurna dan rekod tersebut hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya Perlindungan Data Peribadi.
13.	Memastikan semua kakitangan yang terlibat dalam pemprosesan data peribadi sentiasa menjaga kerahsiaan data peribadi subjek data.
14.	Suatu kontrak perlu diadakan di antara pengguna data dengan pihak yang dilantik oleh pengguna data bagi mengendalikan dan menjalankan aktiviti pemprosesan data peribadi. Ini bagi maksud menjamin keselamatan ke atas data peribadi daripada kehilangan, salah guna, ubahsuaian, akses dan penzahiran tanpa kebenaran.

6.4 Penetapan standard keselamatan bagi data peribadi yang diproses bukan secara elektronik

6.4.1 Pengguna data hendaklah menyediakan langkah-langkah keselamatan yang praktikal ketika pemprosesan data peribadi untuk melindungi data peribadi itu daripada apa-apa kehilangan, salah guna, ubahsuaian, akses atau penzahiran tanpa kebenaran atau tidak sengaja, pengubahan atau pemusnahan dengan mengambil kira faktor berikut:[7]

KESELAMATAN DATA PERIBADI YANG DIPROSES BUKAN SECARA ELEKTRONIK	
Bil.	**Perkara**
1.	Mendaftarkan kakitangan yang menguruskan data peribadi dalam sistem/buku pendaftaran sebelum dibenarkan mengakses data peribadi.
2.	Menamatkan hak akses kakitangan kepada data peribadi selepas kakitangan berhenti kerja, diberhentikan kerja, ditamatkan kontrak atau perjanjian, atau diselaraskan mengikut perubahan dalam organisasi.
3.	Mengawal dan mengehadkan takat kuasa mengakses data peribadi bagi tujuan mengumpul, memproses dan menyimpan data peribadi.
4.	Menetapkan prosedur keselamatan fizikal seperti yang berikut: i. menyimpan semua data peribadi secara teratur dalam fail; ii. menyimpan semua fail yang mengandungi data peribadi di tempat yang berkunci; iii. menyimpan semua kunci yang berkaitan di tempat yang selamat; iv. menyediakan rekod penyimpanan kunci; dan v. menyimpan data peribadi di lokasi yang bersesuaian iaitu selamat daripada ancaman fizikal atau semula jadi serta tidak terdedah.
5.	Menyelenggara rekod akses ke atas data peribadi secara berkala dengan sempurna dan rekod tersebut hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya Perlindungan Data Peribadi.
6.	Memastikan semua kakitangan yang terlibat dalam pemprosesan data peribadi sentiasa menjaga kerahsiaan data peribadi subjek data.

[7] Bahagian II, No. 5, Standard Perlindungan Data Peribadi 2015

7.	Pemindahan data peribadi secara konvensional seperti melalui pos, serahan tangan, faks dan sebagainya hendaklah direkodkan.
8.	Memastikan semua kertas terpakai, dokumen cetakan atau lain-lain dokumen yang jelas menunjukkan data peribadi perlu dimusnahkan dengan teliti dan efisyen seperti menggunakan mesin rincih atau lain-lain kaedah yang bersesuaian.
9.	Mengadakan program kesedaran mengenai tanggungjawab melindungi data peribadi kepada semua kakitangan yang terlibat (sekiranya perlu).

6.5 Pengguna data hendaklah memastikan bahawa standard keselamatan dalam memproses data peribadi dipatuhi oleh mana-mana pemproses data yang menjalankan pemprosesan data peribadi bagi pihak pengguna data itu.[8] Jika pemprosesan data peribadi dijalankan oleh pemproses data bagi pihak pengguna data, adalah disyorkan supaya pengguna data mengambil langkah-langkah yang munasabah untuk memasukkan ke dalam perjanjiannya dengan pemproses data (sama ada dalam bentuk kontrak, surat atau apa-apa bentuk dokumen bertulis rasmi) —

(a) peruntukan mengenai kerahsiaan, ketidakzahiran (*non-disclosure*) dan langkah-langkah keselamatan teknikal dan/atau organisasi;

(b) syarat-syarat di mana data peribadi boleh diproses;

(c) representasi, aku janji, jaminan dan/atau indemniti yang perlu diberikan oleh pemproses data;

(d) langkah-langkah keselamatan yang mengawal pemprosesan yang perlu diambil sebagaimana yang semunasabahnya terkandung dalam polisi dan/atau standard keselamatan dalam pengguna data; dan

[8] Subperaturan 6(3) Peraturan-peraturan Perlindungan Data Peribadi 2013 [*P.U. (A) 335/2013*]

(e) pemadaman, pemusnahan dan/atau pemulangan data peribadi yang berada di bawah kawalan pemproses data apabila kontrak atau pelantikan itu selesai atau tamat, melainkan pengguna data memutuskan sebaliknya.

Contoh: *Kawalan atau langkah-langkah keselamatan perlu dilaksanakan bagi aktiviti pemprosesan yang berisiko tinggi, yang boleh termasuk, tetapi tidak terhad kepada Pengautomatikan Proses Robot (Robot Process Automation (RPA)), kecerdasan buatan (artificial intelligence), analisis data dan teknologi baru yang bakal muncul.*

7. PRINSIP PENYIMPANAN (SEKSYEN 10 AKTA 709)

7.1 Prinsip Penyimpanan mengehadkan pengguna data daripada menyimpan data peribadi untuk diproses lebih lama daripada tujuan ia diperlukan bagi memenuhi tujuan tersebut. Pengguna data boleh menyimpan, menjaga atau memegang data peribadi subjek data sehingga selama yang diperlukan bagi memenuhi tujuan ia dikumpulkan dan berkaitan dengan kehendak-kehendak perniagaan dengan syarat bahawa penyimpanan tersebut adalah dilakukan menurut kehendak undang-undang dan akta yang relevan.

7.2 Peruntukan-peruntukan undang-undang khusus yang lain berhubung penyimpanan data peribadi tidak akan terkesan oleh Prinsip Penyimpanan Akta 709 dan undang-undang lain yang terpakai hendaklah dibaca bersama.

7.3 Penetapan standard penyimpanan bagi data peribadi yang diproses secara elektronik dan data peribadi yang diproses bukan secara elektronik

7.3.1 Pengguna data mengambil 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 dengan[9] —

[9] Bahagian II, No. 6, Standard Perlindungan Data Peribadi 2015

Bil.	Perkara
1.	Menentukan semua perundangan yang berkaitan dengan pemprosesan dan penyimpanan data peribadi dipenuhi sebelum memusnahkan data peribadi.
2.	Tidak menyimpan data peribadi lebih lama daripada yang diperlukan melainkan terdapat peruntukan undang-undang lain yang memerlukan penyimpanan yang lebih lama.
3.	Menyediakan dan menyelenggara rekod pelupusan data peribadi dan rekod tersebut hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya Perlindungan Data Peribadi.
4.	Melupuskan borang pungutan data peribadi yang digunakan untuk transaksi komersial dalam tempoh tidak melebihi empat belas (14) hari, melainkan borang tersebut mempunyai nilai perundangan yang berkaitan dengan transaksi komersial tersebut.
5.	Menyemak dan melupuskan semua data peribadi yang tidak diperlukan di dalam pangkalan data.
6.	Mempunyai jadual pelupusan data peribadi yang tidak aktif bagi tempoh dua puluh empat (24) bulan. Jadual pelupusan data peribadi tersebut perlu diselenggara dengan sempurna.
7.	Penggunaan peranti media mudah alih (*removable media device*) untuk tujuan penyimpanan data peribadi adalah tidak dibenarkan tanpa kebenaran bertulis daripada pengurusan atasan organisasi.

7.4 **Pelupusan data peribadi**

7.4.1 Menjadi kewajipan pengguna 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.[10]

[10] Subseksyen 10(2) Akta 709

7.4.2 Pemusnahan adalah terpakai untuk data peribadi dalam bentuk manual dan pemadaman kekal adalah terpakai untuk data peribadi dalam bentuk elektronik.

7.4.3 Bagi data peribadi yang disimpan dalam medium elektronik, pemadaman kekal data peribadi akan memerlukan media elektronik (seperti pemacu cakera keras atau peranti media mudah alih) dipadamkan sama sekali setelah data peribadi dipadamkan. Pengguna data hendaklah mengambil langkah-langkah munasabah untuk memadamkan secara kekal data peribadi daripada media elektronik.

7.4.4 Sekiranya berlaku pelupusan data, suatu rekod pelupusan perlu disimpan untuk membuktikan tindakan pelupusan tersebut, sebagai contoh buku log, gambar atau kaedah lain yang relevan untuk rekod pelupusan.

8. PRINSIP INTEGRITI DATA (SEKSYEN 11 AKTA 709)

8.1 Penetapan standard integriti data bagi data peribadi yang diproses secara elektronik dan data peribadi yang bukan diproses secara elektronik

8.1.1 Pengguna 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. Langkah-langkah tersebut adalah:[11]

Bil.	Perkara
1.	Menyediakan borang kemas kini data peribadi untuk diisi oleh subjek data sama ada secara dalam talian atau secara konvensional.
2.	Mengemas kini data peribadi dengan segera setelah mendapat notis pembetulan data peribadi daripada subjek data.

[11] Bahagian II, No. 6, Standard Perlindungan Data Peribadi 2015

3.	Memastikan semua perundangan berkaitan dipenuhi dalam menentukan jenis dokumen yang diperlukan bagi menyokong kesahihan data peribadi subjek data.
4.	Memaklumkan mengenai pengemaskinian data peribadi sama ada melalui portal atau mempamerkan pemakluman di premis atau dengan lain-lain kaedah yang bersesuaian.

8.2 Apa yang dimaksudkan sebagai langkah-langkah yang munasabah akan berbeza daripada satu kes kepada kes yang lain, bergantung kepada situasi setiap kes dan juga kepada tujuan dan tujuan yang berkaitan secara langsung dengan perolehan data peribadi.

8.3 Melalui ilustrasi, Akta 709 memerlukan pengguna data mengambil langkah yang munasabah bagi memastikan bahawa data peribadi yang diproses berhubung dengan subjek data —

(a) tepat – bermaksud bahawa data peribadi telah direkodkan dengan betul;

(b) lengkap – bermaksud maklumat berhubung dengan subjek data tidak ditinggalkan;

(c) tidak mengelirukan – bermaksud bahawa data peribadi yang diproses tidak kabur, mengelirukan atau mengandungi kesilapan; dan

(d) dikemaskini ke maklumat terkini – bermaksud data peribadi subjek data harus mencerminkan maklumat disahkan yang terkini berhubung dengan subjek data.

9. PRINSIP AKSES (SEKSYEN 12 AKTA 709)

9.1 Prinsip Akses menghendaki pengguna data untuk memberikan subjek data hak untuk mengakses dan membuat pembetulan ke atas data peribadinya yang didapati tidak tepat, tidak lengkap, mengelirukan atau tidak dikemas kini kecuali di mana pematuhan terhadap permohonan sedemikian untuk mengakses atau membuat pembetulan adalah dihalang di bawah Akta 709.

9.2 **Pematuhan kepada Prinsip Akses**

9.2.1 Dalam mematuhi Prinsip Akses, pengguna data hendaklah memastikan hak subjek data untuk mengakses data peribadi dan untuk membuat pembetulan adalah dilaksanakan menurut Akta 709. Pengguna data boleh menolak hak subjek data untuk mengakses dan/atau untuk membetulkan data peribadinya dengan syarat penolakan itu dilaksanakan menurut Akta 709.

9.3 Fi maksimum yang kena dibayar bagi permintaan mengakses data oleh subjek data, sebagaimana yang disediakan oleh Peraturan-peraturan Perlindungan Data Peribadi (Fi) 2013 [*P.U. (A) 338/2013*] adalah dinyatakan di bawah[12] —

Butiran	Perihalan	Fi maksimum (RM)
1.	Permintaan mengakses data bagi data peribadi subjek data dengan salinan	10
2.	Permintaan mengakses data bagi data peribadi subjek data tanpa salinan	2
3.	Permintaan mengakses data bagi data peribadi sensitif subjek data dengan salinan	30
4.	Permintaan mengakses data bagi data peribadi sensitif subjek data tanpa salinan	5

10. HAK-HAK SUBJEK DATA

10.1 Akta 709 menyediakan data subjek dengan hak-hak seperti yang berikut:

(a) hak untuk mengakses data peribadi;

(b) hak untuk membetulkan data peribadi;

(c) hak untuk menarik balik persetujuan untuk memproses data;

[12] Jadual Pertama, Peraturan 2, Fi Maksimum Permintaan Mengakses Data, Peraturan-peraturan Perlindungan Data Peribadi (Fi) 2013 [*P.U. (A) 338/2013*]

(d) hak untuk menghalang pemprosesan yang mungkin menyebabkan kerosakan atau distres; dan

(e) hak untuk menghalang pemprosesan bagi maksud pemasaran langsung.

10.2 **Hak untuk mengakses data peribadi**

10.2.1 Subjek data mempunyai hak untuk memohon akses kepada data peribadinya yang diproses oleh atau bagi pihak pengguna data dan mempunyai hak untuk membuat Permintaan Akses Data ("PAD") kepada pengguna data dan untuk mendapat maklum balas daripada pengguna data dalam tempoh masa yang ditetapkan mengikut Akta 709. Bagi mengelakkan kekeliruan, mana-mana data peribadi yang disimpan untuk tujuan sandaran adalah tidak tertakluk untuk diakses oleh subjek data.

10.2.2 Adalah disyorkan supaya pengguna data menyediakan suatu Borang PAD di tempat-tempat yang sesuai dan mudah untuk diperolehi di premis perniagaan pengguna data apabila diperlukan oleh subjek data semasa mengemukakan permohonan. Pengguna data boleh merujuk kepada sampel templat Borang PAD yang dilampirkan sebagai **Lampiran 2**.

10.2.3 **Pematuhan pengguna data terhadap PAD**

Pengguna data hendaklah mematuhi PAD dengan —

(a) memastikan pembayaran fi yang telah ditetapkan selaras dengan Jadual Pertama, Peraturan-peraturan Perlindungan Data Peribadi (Fi) 2013 [*P.U. (A) 338/2013*] dijelaskan oleh subjek data. Adalah dinasihatkan bahawa fi yang perlu dibayar bagi pengemukaan PAD dinyatakan dalam Borang PAD;

(b) menyediakan borang yang seragam untuk permohonan kebenaran akses kepada data peribadi;

(c) menyediakan kepada peminta satu salinan data peribadi subjek data dalam apa juga bentuk selagi mana ia boleh difahami oleh peminta dalam tempoh dua puluh satu (21) hari dari tarikh penerimaan permintaan mengakses data;

(d) sekiranya pengguna data tidak dapat mematuhi PAD dalam tempoh dua puluh satu (21) hari, pengguna data adalah dikehendaki untuk memaklumkan peminta melalui notis bertulis sebab-sebab dia tidak boleh berbuat demikian dan selanjutnya mematuhi PAD setakat yang dia boleh berbuat demikian; dan

(e) mematuhi PAD keseluruhannya tidak lewat daripada empat belas (14) hari selepas habis tempoh dua puluh satu (21) hari.

10.2.4 **Keengganan pengguna data untuk mematuhi PAD**

Pengguna data mempunyai hak untuk tidak mematuhi PAD sekiranya —

(a) identiti tidak boleh disahkan. Pengguna data tidak dibekalkan dengan maklumat yang diperlukan untuk memastikan identiti subjek data atau sekiranya PAD dihantar adalah bagi pihak, untuk memastikan kaitan peminta dengan subjek data;

(b) pengguna data tidak disediakan dengan maklumat yang mencukupi untuk mengesan data peribadi yang dengannya permintaan mengakses data itu adalah berhubungan;

(c) beban yang tidak setimpal. Beban atau perbelanjaan untuk menyediakan akses kepada data peribadi adalah tidak setimpal dengan risiko kepada privasi subjek data sebagai contoh sekiranya masa dan kos yang digunakan adalah lebih besar daripada memenuhi permohonan PAD;

(d) penzahiran yang lain. Pengguna data tidak dapat mematuhi PAD tanpa menzahirkan data peribadi subjek data yang lain. Dalam keadaan demikian, pengguna data boleh menzahirkan sama ada secara tanpa nama data peribadi subjek data yang lain atau mendapatkan persetujuan daripada subjek data itu, atau mana-mana cara praktikal yang lain untuk menzahirkan data peribadi tanpa melanggar Akta 709;

(e) memberikan akses akan menjadi pelanggaran suatu perintah mahkamah;

(f) memberikan akses akan menzahirkan maklumat komersial yang sulit; atau

(g) apa-apa akses kepada data peribadi itu dikawal selia oleh undang-undang lain.

10.3 **Hak untuk membetulkan data peribadi**

10.3.1 Subjek data adalah berhak untuk memohon data peribadi yang dipegang oleh pengguna data supaya dibetulkan sekiranya dia berpuas hari bahawa data peribadi itu tidak tepat, tidak lengkap, mengelirukan atau tidak terkini dengan mengemukakan Permintaan Pembetulan Data ("PPD").

10.3.2 Adalah disyorkan supaya pengguna data menyediakan suatu Borang PPD di tempat-tempat yang sesuai dan mudah untuk diperolehi di premis perniagaan pengguna data apabila diperlukan oleh subjek data semasa mengemukakan permohonan. Pengguna data boleh merujuk kepada sampel templat Borang PPD yang dilampirkan sebagai **Lampiran 3**.

10.3.3 **Keabsahan PPD**

Dalam memastikan bahawa PPD adalah sah, pengguna data adalah diminta untuk memastikan bahawa —

(a) PPD dibuat secara bertulis;

(b) PPD adalah spesifik kepada data peribadi yang hendak dibetulkan;

(c) PPD mempunyai maklumat yang diperlukan dengan dokumen yang disahkan untuk mengenal pasti identiti peminta dan sekiranya peminta bukanlah subjek data, memastikan hak dan identiti peminta dan kaitan dengan subjek data;

(d) pengguna data diberi maklumat sebagaimana yang dikehendaki dengan munasabah olehnya untuk memastikan bentuk cara data peribadi yang hendak dibetulkan adalah tidak tepat, tidak lengkap, mengelirukan dan tidak terkini;

(e) pengguna data berpuas hati bahawa pembetulan yang menjadi subjek permohonan pembetulan adalah tidak tepat, tidak lengkap, mengelirukan dan tidak terkini; dan

(f) pengguna data mempunyai kuasa dalam pemprosesan data peribadi yang memerlukan pembetulan dan tidak dihalang oleh lain-lain pengguna data untuk mematuhi PPD.

10.3.4 **Pematuhan pengguna data terhadap PPD**

Pengguna data hendaklah mematuhi PPD tidak lewat daripada dua puluh satu (21) hari dari tarikh penerimaan PPD dengan —

(a) membuat pembetulan yang perlu kepada data peribadi;

(b) memberi peminta suatu salinan data peribadi yang telah dibetulkan;

(c) mengambil segala langkah praktikal untuk memberi pihak ketiga suatu salinan data peribadi yang telah dibetulkan berserta dengan suatu notis bertulis yang menyatakan sebab-sebab bagi pembetulan itu;

(d) sekiranya pengguna data tidak dapat mematuhi PPD dalam tempoh dua puluh satu (21) hari dari tarikh penerimaan PPD, hendaklah sebelum habis tempoh itu —

(i) melalui notis bertulis memaklumkan peminta bahawa dia tidak dapat mematuhi PPD dalam tempoh itu dan sebab-sebab kenapa dia tidak dapat berbuat demikian; dan

(ii) mematuhi PPD itu ke apa-apa takat yang dapat dibuat olehnya; dan

(e) mematuhi keseluruhan PPD itu tidak lewat daripada empat belas (14) hari selepas habis tempoh dua puluh satu (21) hari.

10.3.5 Keengganan pengguna data untuk mematuhi PPD

Pengguna data mempunyai hak untuk tidak mematuhi PPD sekiranya —

(a) identiti tidak boleh disahkan. Pengguna data tidak dibekalkan dengan maklumat yang diperlukan untuk memastikan identiti subjek data atau sekiranya PPD dihantar adalah bagi pihak, untuk memastikan kaitan peminta dengan subjek data;

(b) tidak boleh mengenal pasti keperluan untuk pembetulan. Pengguna data tidak dibekalkan dengan maklumat secukupnya yang sewajarnya untuk memastikan bentuk cara data peribadi yang hendak dibetulkan adalah tidak tepat, tidak lengkap, mengelirukan dan tidak terkini;

(c) pengguna data tidak berpuas hati bahawa data peribadi yang dengannya PPD adalah berhubungan adalah tidak tepat, tidak lengkap, mengelirukan dan tidak terkini; atau

(d) pengguna data tidak berpuas hati bahawa pembetulan yang dipohon adalah tepat, lengkap, tidak mengelirukan dan terkini.

10.4 **Hak untuk menarik balik persetujuan untuk memproses data peribadi**

10.4.1 Subjek data boleh melalui notis bertulis menarik balik persetujuannya terhadap pemprosesan data peribadi yang berkenaan dengannya dia merupakan subjek data.[13]

10.4.2 Pengguna data hendaklah, apabila menerima notis berhenti memproses data peribadi kecuali sehingga penolakan persetujuan akan menjejaskan hak dan tanggungjawab pengguna data di bawah kontrak atau undang-undang. Contoh hak dan tanggungjawab itu termasuk —

(a) hak untuk dibayar kepada perkhidmatan yang telah diberikan, sebagai contoh, penyelesaian tempahan atau invois cukai atau bayaran tertunggak;

(b) hak untuk membawa dan mengekalkan prosiding undang-undang terhadap subjek data;

(c) hak untuk memulakan dan meneruskan penyiasatan dalaman yang melibatkan subjek data;

(d) tanggungjawab untuk mengekalkan data peribadi untuk jangka masa sebagaimana yang dikehendaki di bawah undang-undang yang berkaitan; dan

(e) pengendalian audit dalaman, pengurusan risiko dan/atau memenuhi keperluan undang-undang atau keperluan melaporkan pengawalseliaan.

[13] Subseksyen 38(1) Akta 709

10.5 **Hak untuk menghalang pemprosesan yang mungkin menyebabkan kerosakan atau distres**

10.5.1 Data subjek boleh, pada bila-bila masa melalui notis bertulis kepada pengguna data, menghendaki pengguna data untuk —

(a) memberhentikan pemprosesan data peribadi; atau

(b) tidak memulakan pemprosesan data peribadi,

di mana pemprosesan data peribadi itu menyebabkan atau mungkin menyebabkan kerosakan atau distres yang substansial atau akan menjadi tidak wajar kepadanya atau kepada orang lain.

10.5.2 **Kehendak**

Subjek data adalah dikehendaki untuk membuktikan bahawa —

(a) pemprosesan data peribadi itu atau pemprosesan data peribadi untuk tujuan atau cara yang mungkin menyebabkan kerosakan yang substansial atau distres yang substansial kepadanya atau kepada orang lain; dan

(b) kerosakan atau distres menjadi atau akan menjadi tidak wajar.

Dalam kebanyakan kes —

(a) “kerosakan substansial” termasuk kerugian kewangan yang dialami oleh subjek data atau orang lain;

(b) “distres substansial” termasuk kesengsaraan emosi atau mental yang dialami oleh subjek data atau orang lain; dan

(c) “tidak wajar” bermaksud kerosakan atau distres yang dialami oleh subjek data atau orang lain yang tidak boleh dijustifikasikan.

10.5.3 Keadaan-keadaan di mana subjek data tiada hak menghalang pemprosesan

Subjek data hendaklah tidak mempunyai hak untuk menghalang pemprosesan di mana —

(a) subjek data telah memberikan persetujuan untuk pemprosesan; atau

(b) pemprosesan data peribadi itu perlu —
   (i) bagi melaksanakan suatu kontrak yang mengenainya subjek data itu merupakan suatu pihak;
   (ii) bagi mengambil langkah, atas permintaan subjek data, dengan tujuan untuk membuat suatu kontrak;
   (iii) bagi mematuhi apa-apa obligasi undang-undang yang mengenainya pengguna data itu merupakan subjek, selain suatu obligasi yang dikenakan oleh kontrak; atau
   (iv) untuk melindungi kepentingan vital subjek data itu.

10.5.4 Pematuhan pengguna data terhadap hak untuk menghalang pemprosesan yang mungkin menyebabkan kerosakan atau distres

Setelah menerima notis bertulis untuk menghentikan pemprosesan atau tidak memulakan pemprosesan data peribadi, pengguna data hendaklah, dalam tempoh dua puluh satu (21) hari, memberi subjek data suatu notis bertulis menyatakan —

(a) bahawa pengguna data telah mematuhi atau berhasrat untuk mematuhi notis subjek data itu;

(b) sekiranya pengguna data enggan memenuhi notis subjek data, menyatakan sebab untuk keputusan itu; atau

(c) menyatakan sebab mengapa notis subjek data tersebut dianggap oleh pengguna data sebagai tidak wajar setakat yang tertentu, dan setakat mana pengguna data telah mematuhi atau berhasrat untuk mematuhinya (jika ada).

Pengguna data boleh mempertimbangkan perkara seperti yang berikut apabila membuat keputusan sama ada untuk mematuhi permintaan itu —

(a) adakah permintaan subjek data untuk tujuan yang sah? Subjek data harus memberikan sebab-sebab yang sah kerana kerosakan atau distres yang terjadi adalah substansial; dan

(b) adakah kerosakan atau distres tidak wajar? Ini berhubung kait sama ada subjek data telah memberikan sebab-sebab yang sah untuk permintaan itu.

Di mana pengguna data tidak mematuhi notis itu, subjek data boleh memohon kepada Pesuruhjaya Perlindungan Data Peribadi untuk meminta pengguna data mematuhi notis itu. Jika Pesuruhjaya Perlindungan Data Peribadi berpuas hati bahawa permintaan subjek data adalah wajar, Pesuruhjaya Perlindungan Data Peribadi boleh mengarahkan pengguna data untuk mematuhi permintaan tersebut.

10.6 Hak untuk menghalang pemprosesan bagi maksud pemasaran langsung

10.6.1 Selaras dengan Akta 709, subjek data mempunyai hak pada bila-bila masa melalui notis bertulis kepada pengguna data, menghendaki pengguna data itu untuk memberhentikan atau tidak memulakan pemprosesan data peribadinya bagi maksud pemasaran langsung. Pengguna data boleh merujuk kepada sampel templat notis di bawah Subseksyen 43(1) Akta 709 yang dilampirkan sebagai **Lampiran 4**.

10.6.2 Pengguna data hendaklah mematuhi permintaan itu dalam tempoh masa yang munasabah.

10.6.3 Pengguna data yang menyampaikan bahan pengiklanan atau pemasaran yang ditujukan kepada subjek data tertentu, melalui penggunaan data peribadi subjek data, adalah dikehendaki sama ada untuk sudah memaklumkan subjek data melalui Notis PDP, atau dalam keadaan di mana Notis PDP tidak menyebut mengenai pengeluaran bahan pengiklanan atau pemasaran, untuk mendapat kebenaran subjek data sebelum memulakan pemasaran langsung.

10.6.4 Pengguna data dibenarkan untuk menjalankan pemasaran langsung kepada subjek data —

(a) jika persetujuan telah diperolehi daripada subjek data;

(b) untuk pengumpulan data peribadi bagi penjualan produk atau penyediaan perkhidmatan;

(c) jika subjek data telah dimaklumkan mengenai identiti organisasi pemasaran langsung dan maksud pengumpulan dan penzahiran;

(d) jika produk dan/atau perkhidmatan yang ditawarkan kepada subjek data adalah serupa dengan produk dan perkhidmatan yang disediakan secara am oleh pengguna data; atau

(e) sekiranya pengguna data komited untuk menyediakan pilihan pilih-keluar (*opt-out*) kepada subjek data semasa pengumpulan data peribadi.

10.6.5 Di mana subjek data membuat permintaan secara bertulis memohon untuk menerima beberapa bahan pemasaran langsung dan bukan yang lain, pengguna data boleh memilih untuk tidak memberikan subjek data dengan semua bahan pemasaran langsung, sekiranya sistemnya tidak berupaya untuk membezakan antara jenis bahan pemasaran yang berlainan.

10.6.6 Jika subjek data tidak berpuas hati bahawa pengguna data gagal untuk mematuhi keseluruhan atau sebahagian notis bertulis, subjek data boleh mengemukakan permohonan kepada Pesuruhjaya Perlindungan Data Peribadi untuk menghendaki pengguna data untuk mematuhinya. Kegagalan pengguna data untuk mematuhi kehendak Pesuruhjaya Perlindungan Data Peribadi merupakan suatu kesalahan yang boleh dikenakan hukuman denda tidak melebihi dua ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya[14].

11. PEMATUHAN DAN PEMANTAUAN TATAAMALAN UMUM PERLINDUNGAN DATA PERIBADI

11.1 Sistem data peribadi hendaklah pada sepanjang masa yang munasabah terbuka untuk diperiksa oleh Pesuruhjaya Perlindungan Data Peribadi atau mana-mana pegawai pemeriksa.[15]

11.2 Pengguna data hendaklah mengekalkan —

(a) berhubung dengan Prinsip Am, rekod persetujuan daripada subjek data yang disenggara berkenaan dengan pemprosesan data peribadi oleh pengguna data;

(b) berhubung dengan Prinsip Notis dan Pilihan, rekod notis bertulis yang dikeluarkan oleh pengguna data kepada subjek data mengikut Seksyen 7 Akta 709;

(c) berhubung dengan Prinsip Penzahiran, senarai penzahiran kepada pihak ketiga bagi maksud perenggan 8*(b)* Akta 709 berkenaan dengan data peribadi yang telah atau sedang diproses olehnya;

(d) berhubung dengan Prinsip Keselamatan, polisi keselamatan yang dibangunkan dan dilaksanakan oleh pengguna data bagi maksud Seksyen 9 Akta 709;

[14] Subseksyen 42(6) Akta 709
[15] Subperaturan 14(1) Peraturan-peraturan Perlindungan Data Peribadi 2013 [*P.U. (A) 335/2013*]

(e) berhubung dengan Prinsip Penyimpanan, rekod pematuhan mengikut standard penyimpanan;

(f) berhubung dengan Prinsip Integriti Data, rekod pematuhan mengikut standard integriti data; atau

(g) apa-apa maklumat lain yang berkaitan yang disifatkan perlu oleh Pesuruhjaya Perlindungan Data Peribadi atau pegawai pemeriksa.

11.3 Pengguna data adalah dikehendaki untuk membangunkan dan melaksanakan polisi dan prosedur pematuhan (rangka kerja pematuhan) yang bersesuaian untuk memastikan pematuhan kepada Tataamalan Umum Perlindungan Data Peribadi, Akta 709, peraturan-peraturan dan standard.

11.4 Adalah disyorkan supaya pengguna data memantau pematuhan kepada Tataamalan Umum Perlindungan Data Peribadi, Akta 709, peraturan-peraturan dan standard secara berterusan dengan —

(a) melaksanakan pemantauan rangka kerja dalaman; dan

(b) menjalankan audit.

11.5 Pengguna data adalah digalakkan untuk memastikan latihan dan/atau kesedaran yang bersesuaian disediakan untuk setiap kakitangan bagi memastikan kakitangan memahami kepentingan untuk mematuhi polisi dan prosedur tersebut. Kakitangan yang berkaitan akan dikenal pasti untuk menerima latihan khusus, seperti latihan keselamatan dan kesedaran penipuan dan mengendalikan akses data/permohonan pembetulan.

11.6 Pengguna data adalah dikehendaki untuk memastikan bahawa dia mengikuti perkembangan terkini berkenaan Akta 709 dan sentiasa memberikan latihan kepada kakitangan apabila diperlukan untuk terus mengikuti sebarang perubahan.

12. KEHENDAK UNTUK MENYEDIAKAN TATAAMALAN BAGI SUATU GOLONGAN PENGGUNA DATA YANG KHUSUS

12.1 Sesuatu badan yang dinamakan oleh Pesuruhjaya Perlindungan Data Peribadi sebagai suatu forum pengguna data yang khusus hendaklah menyediakan Tataamalan bagi suatu Golongan Pengguna Data yang khusus dalam tempoh dua (2) tahun dari tarikh penamaan.

12.2 Pesuruhjaya Perlindungan Data Peribadi boleh membatalkan, meminda atau menyemak, sama ada keseluruhannya atau sebahagiannya, mana-mana Tataalaman yang didaftarkan di bawah Akta 709 selaras dengan Seksyen 26 Akta 709.

Lampiran 1

Notis Perlindungan Data Peribadi

[Logo / Nama Perniagaan]

(Berkuat kuasa pada: hh bb tt)
(Terakhir dikemas kini pada: hh bb tt)

PENGENALAN

(Nama perniagaan) mengambil berat mengenai perlindungan data peribadi anda. Notis ini menjelaskan bagaimana (nama perniagaan) memproses data peribadi anda bermula daripada pengumpulan, penggunaan, perkongsian dan pemusnahan serta langkah keselamatan yang kami ambil untuk memastikan data peribadi anda dilindungi sebaiknya.

PENGUMPULAN

Kami mengumpul data peribadi iaitu nama, alamat rumah, alamat e-mel, nombor telefon dan nombor akaun anda. [Tambah / ubah senarai ini ikut kesesuaian]

SUMBER PENGUMPULAN

Kami mendapatkan data peribadi anda daripada:

1. Borang pendaftaran ahli baru di laman sesawang xxx (namakan)
2. Borang pembelian
3. *Cookies*
4. [Tambah / ubah senarai ini ikut kesesuaian]

TUJUAN PENGUMPULAN

Kami mengumpul data peribadi anda untuk:

1. Memproses permohonan anda untuk membeli produk / servis kami
2. Menghantar produk kami ke lokasi pilihan anda
3. Menyelesaikan aduan / masalah penghantaran (sekiranya berlaku)
4. Menghantar pemasaran produk baru kepada anda (dengan persetujuan baru)
5. [Tambah / ubah senarai ini ikut kesesuaian]

BAGAIMANA DIPROSES

Kami memproses data peribadi anda hanya di dalam Malaysia sahaja. Tiada data peribadi yang dipindahkan ke luar Malaysia. [Ubah ikut kesesuaian]

PENZAHIRAN

Kami akan menzahirkan data peribadi anda kepada:

1. Pihak kurier dilantik bagi menghantar produk yang dibeli oleh anda
2. Pihak berkuasa untuk tujuan undang-undang (nyatakan pihak berkaitan)
3. [Tambah / ubah senarai ini ikut kesesuaian]

LANGKAH KESELAMATAN

Kami mengambil langkah-langkah berikut untuk melindungi data peribadi anda:

1. Memastikan data peribadi anda disimpan dengan sebaiknya mengikut kehendak Akta 709
2. Memastikan kakitangan kami tidak menyalah gunakan data peribadi anda
3. Mempunyai kontrak perlindungan data peribadi dengan pihak pembekal sistem / kurier dilantik.
4. [Tambah / ubah senarai ini ikut kesesuaian]

Walau bagaimanapun, anda bertanggungjawab untuk menjaga kata laluan dengan baik dan tidak menzahirkannya kepada pihak lain bagi mengelakkan risiko pencerobohan terhadap data peribadi anda.

TEMPOH PENYIMPANAN

Kami akan menyimpan data peribadi anda selama tujuh (7) tahun / selagi anda menjadi pelanggan kami [Ubah ikut kesesuaian]. Sekiranya anda tidak lagi menjadi pelanggan kami, data peribadi anda akan dihapuskan secara kekal.

HAK ANDA

Anda berhak untuk:

1. Membetulkan / mengemas kini data peribadi anda (pautan borang pembetulan data peribadi)
2. Mengakses data peribadi anda yang kami simpan

3. Menghentikan promosi produk kami kepada anda
4. Menarik balik persetujuan memproses data peribadi [Nyatakan kesan daripada tindakan subjek data ini].

HUBUNGI KAMI

Anda boleh menghubungi kami berkaitan data peribadi anda melalui:

(Nama)

(Jawatan)

(Alamat)

(No. Telefon)

(No. Faks / alamat e-mel)

Lampiran 2

AKTA PERLINDUNGAN DATA PERIBADI 2010 [*AKTA 709*]
BORANG PERMINTAAN AKSES DATA PERIBADI

Maklumat berikut diperlukan bagi membantu kami memberikan maklum balas yang cepat dan tepat kepada Permintaan Akses Data Peribadi anda menurut Akta 709.

Nama Penuh Subjek Data atau Orang Yang Berkaitan	
Hubungan Orang Yang Berkaitan dengan Subjek Data	
Alamat	
Nombor Telefon Mudah Alih	
Alamat E-mel	
Sila nyatakan butiran maklumat yang anda kehendaki daripada [Pengguna Data]:	

Pengisytiharan: Saya Subjek Data / Orang Yang Berkaitan yang dinyatakan di atas dengan ini meminta, di bawah peruntukan Seksyen 12 dan 30 Akta Perlindungan Data Peribadi 2010 [*Akta 709*], bahawa [**Pengguna Data**] membekalkan saya dengan salinan data peribadi saya yang disimpan seperti di atas. Saya memahami bahawa bayaran untuk perkhidmatan ini mungkin dikenakan dan [**Pengguna Data**] akan menghubungi saya untuk membuat tuntutan bayaran tersebut. Saya juga ambil maklum bahawa [**Pengguna Data**] akan memberi maklum balas dalam tempoh yang dinyatakan dalam Akta 709 selepas menerima pembayaran daripada saya dan akan memaklumkan kepada saya tarikh dan waktu untuk hadir sendiri bagi tujuan pengambilan salinan dokumen itu.

Tandatangan …… Tarikh ……

Lampiran 3

<table>
<tr><th colspan="2">BORANG PERMINTAAN PEMBETULAN DATA PERIBADI</th></tr>
<tr><td colspan="2">• Kami berhak untuk mengehadkan atau menolak akses kepada butiran data peribadi seperti yang dibenarkan Akta Perlindungan Data 2010 [Akta 709].
• Permohonan ini tidak diproses sekiranya maklumat dan dokumen tidak lengkap.
• Permintaan Pembetulan Data Peribadi hendaklah disertakan dengan bukti bila perlu.
• Hendaklah diisi dengan HURUF BESAR.</td></tr>
<tr><td colspan="2">Sila tandakan (√) mana yang berkenaan:
☐ Akses maklumat peribadi sendiri
(Sila isikan Seksyen 1 dan Seksyen 3 di bawah)
☐ Saya merupakan Peminta Pihak Ketiga
(Sila isikan Seksyen 1 dan Seksyen 3 di bawah)</td></tr>
<tr><td colspan="2">SEKSYEN 1 : DIISI OLEH SUBJEK DATA</td></tr>
<tr><td>Nama Penuh
(seperti Kad Pengenalan/ Pasport)</td><td></td></tr>
<tr><td>No. Kad Pengenalan/Pasport</td><td></td></tr>
<tr><td>No. Telefon Mudah Alih</td><td></td></tr>
<tr><td colspan="2">SEKSYEN 2: DIISI OLEH PEMINTA PIHAK KETIGA (ORANG YANG DIBERI KUASA)
Permohonan ini adalah berdasarkan (sila tandakan (√) satu daripada yang berikut):
☐ Saya bertindak dengan kuasa/mandat daripada Subjek Data/Surat Kuasa Wakil
☐ Saya merupakan wakil sah/peribadi Subjek Data
☐ Saya mempunyai Waran atau Perintah Mahkamah yang membenarkan pembetulan kepada data peribadi Subjek Data
☐ Saya merupakan pelaksana/pentadbir estet Subjek Data
☐ Lain-lain (sila nyatakan)
…….

Sila lampirkan bukti autoriti untuk membetulkan data peribadi Subjek Data</td></tr>
</table>

A : Butiran Subjek Data	
Nama Penuh (seperti Kad Pengenalan/ Pasport)	
No. Kad Pengenalan/Pasport	
No. Telefon Mudah Alih	
B: Butiran Pemohon (selain Subjek Data)	
Nama Penuh (seperti Kad Pengenalan/ Pasport)	
No. Kad Pengenalan/Pasport	
No. Telefon Mudah Alih	
Alamat E-mel	
Alamat Surat-menyurat	
SEKSYEN 3 : PEMBETULAN DATA PERIBADI (Sila tandakan (√) dan sila isi Seksyen yang relevan sahaja)	
□ Nama Penuh (seperti Kad Pengenalan/ Pasport)	
□ No. Kad Pengenalan/Pasport	
□ Alamat premis	
□ No. Telefon Mudah Alih	
□ Alamat Surat-menyurat	
□ *No. Telefon Rumah	
□ *No. Telefon Pejabat	
**Tidak wajib diisi*	

DEKLARASI	
Pengesahan Subjek Data Saya,…… penama di Seksyen 1 dan memohon bagi pihak saya sendiri. Saya mengesahkan bahawa semua maklumat yang diberikan adalah benar dan tepat. Tandatangan:…… Tarikh: ……	**Pengesahan Pemohon (Selain Subjek Data)** Saya,…….. penama di Seksyen 2 dan memohon sebagai pihak yang telah diberi kuasa oleh Subjek Data. Saya mengesahkan bahawa semua maklumat yang diberikan adalah benar dan tepat. Tandatangan: …… Tarikh: ……

UNTUK KEGUNAAN PEJABAT SAHAJA (sila isi Seksyen yang relevan sahaja)	
□ DILULUSKAN TARIKH DIKEMAS KINI: DIURUSKAN OLEH:	□ TIDAK DILULUSKAN ALASAN: TARIKH NOTIFIKASI: DIURUSKAN OLEH:

Lampiran 4

NOTIS DI BAWAH SUBSEKSYEN 43(1)

AKTA PERLINDUNDAN DATA PERIBADI 2010 [*AKTA 709*]

Tarikh:

Alamat Pengguna Data:

..……

..……

Tuan / Puan,

NOTIS DI BAWAH SUBSEKSYEN 43(1) AKTA PERLINDUNGAN DATA PERIBADI 2010 [*AKTA 709*] UNTUK MENGHALANG PEMPROSESAN DATA PERIBADI BAGI MAKSUD PEMASARAN LANGSUNG

Saya, …… (nama penuh) …… (No. Kad Pengenalan/Pasport) menghendaki tuan/puan untuk memberhentikan atau tidak memulakan pemprosesan data peribadi saya bagi maksud pemasaran langsung dalam tempoh _____ * dari tarikh penerimaan notis ini.

Sekian, terima kasih.

Tandatangan: ..……

Nama: ..……..

Alamat: ..…….

..……

..……

No. Telefon: ..…….

E-mel: ..……..

*Subjek data boleh menentukan tempoh masa yang dirasakan munasabah

Lampiran 5

SENARAI KESALAHAN DAN HUKUMAN DI BAWAH AKTA PERLINDUNGAN DATA PERIBADI 2010 [*AKTA 709*] DAN PERUNDANGAN SUBSIDIARI

BIL.	SEKSYEN / PERATURAN	KESALAHAN	HUKUMAN
1.	Subseksyen 5(2) Prinsip-prinsip Perlindungan Data Peribadi	Ketidakpatuhan pemprosesan data peribadi di bawah Prinsip-prinsip Perlindungan Data Peribadi	Denda tidak melebihi RM300,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
2.	Subseksyen 16(4) Perakuan pendaftaran	Memproses data peribadi tanpa suatu perakuan pendaftaran yang dikeluarkan di bawah perenggan 16(1)*(a)*	Denda tidak melebihi RM500,000 atau dipenjarakan selama tempoh tidak melebihi tiga (3) tahun atau kedua-duanya
3.	Subseksyen 18(4) Pembatalan pendaftaran	Memproses data peribadi selepas pendaftaran dibatalkan	Denda tidak melebihi RM500,000 atau dipenjarakan selama tempoh tidak melebihi tiga (3) tahun atau kedua-duanya
4.	Subseksyen 19(2) Penyerahan perakuan pendaftaran	Kegagalan untuk menyerahkan perakuan pendaftaran kepada Pesuruhjaya Perlindungan Data Peribadi selepas ia dibatalkan	Denda tidak melebihi RM200,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
5.	Seksyen 29 Ketidakpatuhan Tataamalan	Ketidakpatuhan mana-mana peruntukan Tataamalan yang terpakai bagi pengguna data	Denda tidak melebihi RM100,000 atau dipenjarakan selama tempoh tidak melebihi satu (1) tahun atau kedua-duanya

6.	Subseksyen 37(4) Pemberitahuan mengenai keengganan untuk mematuhi permintaan pembetulan data	Ketidakpatuhan mana-mana peruntukan di bawah subseksyen 37(2)	Denda tidak melebihi RM100,000 atau dipenjarakan selama tempoh tidak melebihi satu (1) tahun atau kedua-duanya
7.	Subseksyen 38(4) Penarikan balik persetujuan untuk memproses data peribadi	Terus memproses data peribadi selepas penarikan balik persetujuan oleh subjek data	Denda tidak melebihi RM100,000 atau dipenjarakan selama tempoh tidak melebihi satu (1) tahun atau kedua-duanya
8.	Subseksyen 40(3) Pemprosesan data peribadi sensitif	Pemprosesan data peribadi sensitif tanpa mematuhi syarat-syarat di bawah subseksyen 40(1)	Denda tidak melebihi RM200,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
9.	Subseksyen 42(6) Hak untuk menghalang pemprosesan yang mungkin menyebabkan kerosakan atau distres	Ketidakpatuhan kehendak Pesuruhjaya Perlindungan Data Peribadi di bawah subseksyen 42(5)	Denda tidak melebihi RM200,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
10.	Subseksyen 43(4) Hak untuk menghalang pemprosesan bagi maksud pemasaran langsung	Ketidakpatuhan kehendak Pesuruhjaya Perlindungan Data Peribadi di bawah subseksyen 43(3)	Denda tidak melebihi RM200,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
11.	Subseksyen 108(8) Notis penguatkuasaan	Ketidakpatuhan suatu notis penguatkuasaan	Denda tidak melebihi RM200,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya

12.	Subseksyen 113(7) Penggeledahan dan penyitaan dengan waran	Seseorang yang tanpa kuasa yang sah, memecahkan, mengganggu atau merosakkan lak (*seal*) yang disebut dalam subseksyen 113(6) atau memindahkan mana-mana computer, buku, akaun, data berkomputer atau dokumen lain, papan tanda, kad, surat, risalah, lembaran, notis, kelengkapan, peralatan atau barang yang dilak atau cuba untuk berbuat demikian	Denda tidak melebihi RM50,000 atau dipenjarakan selama tempoh tidak melebihi enam (6) bulan atau kedua-duanya
13.	Seksyen 120 Halangan terhadap penggeledahan	Mana-mana orang yang — (a) enggan memberi akses kepada pegawai berkuasa; (b) mengamang (*assaults*), menghalang, menggalang (*hinders*) atau melengahkan mana-mana pegawai berkuasa; atau (c) enggan memberi maklumat kepada mana-mana pegawai diberi kuasa apa-apa maklumat berhubungan dengan sesuatu kesalahan atau kesalahan yang disyaki	Dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau didenda tidak melebihi RM10,000 atau kedua-duanya

14.	Subseksyen 129(5) Pemindahan data peribadi ke tempat di luar Malaysia	Ketidakpatuhan kehendak dalam subseksyen 129(1) — memindahkan data peribadi mengenai seorang subjek data ke suatu tempat di luar Malaysia, selain tempat yang ditentukan oleh Menteri, atas syor Pesuruhjaya Perlindungan Data Peribadi, melalui pemberitahuan yang disiarkan dalam *Warta*	Denda tidak melebihi RM300,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
15.	Subseksyen 130(7) Pengumpulan, dsb., data peribadi yang menyalahi undang-undang	Melakukan kesalahan seperti yang dinyatakan di bawah seksyen 130	Denda tidak melebihi RM500,000 atau dipenjarakan selama tempoh tidak melebihi tiga (3) tahun atau kedua-duanya
16.	Subseksyen 131(1) dan (2) Persubahatan dan cubaan boleh dihukum sebagai kesalahan	Subseksyen 131(1) Bersubahat dalam pelakuan atau yang cuba untuk melakukan apa-apa kesalahan di bawah Akta 709	Dengan syarat bahawa apa-apa tempoh pemenjaraan yang dikenakan tidak melebihi setengah daripada tempoh maksimum yang diperuntukkan bagi kesalahan itu
		Subseksyen 131(2) Melakukan apa-apa perbuatan sebagai persediaan untuk melakukan atau sebagai pelanjutan kepada pelakuan mana-mana kesalahan di bawah Akta 709	Dengan syarat bahawa apa-apa tempoh pemenjaraan yang dikenakan tidak melebihi setengah daripada tempoh maksimum yang diperuntukkan bagi kesalahan itu

17.	Subseksyen 141(2) Obligasi kerahsiaan	Kesalahan di bawah perenggan 141(1)*(a)* dan *(b)* — Pesuruhjaya Perlindungan Data Peribadi, pegawai atau pekhidmatnya, mana-mana anggota, pegawai atau pekhidmat Tribunal Rayuan, mana-mana pegawai diberi kuasa atau mana-mana orang yang menghadiri mana-mana mesyuarat atau pertimbangtelitian Jawatankuasa Penasihat, sama ada semasa atau selepas tempoh jawatan atau penggajiannya, pada bila-bila masa, tidak boleh menzahirkan apa-apa maklumat yang diperoleh olehnya semasa menjalankan kewajipannya	Denda tidak melebihi RM100,000 atau dipenjarakan selama tempoh tidak melebihi satu (1) tahun atau kedua-duanya
18.	Subseksyen 143(3) Kuasa untuk membuat peraturan-peraturan	Ketidakpatuhan apa-apa peraturan-peraturan atau perundangan subsidiari lain di bawah seksyen ini	Denda tidak melebihi RM250,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
PERATURAN-PERATURAN PERLINDUNGAN DATA PERIBADI 2013 [*P.U. (A) 335/2013*]			
1.	Peraturan 12 Penalti	Ketidakpatuhan dengan yang berikut: • subperaturan 3(1)	Denda tidak melebihi RM250,000 atau dipenjarakan selama tempoh tidak melebihi

		persetujuan subjek data • peraturan 6 polisi keselamatan • peraturan 7 standard penyimpanan • peraturan 8 • standard data integriti	dua (2) tahun atau kedua-duanya
PERATURAN-PERATURAN PERLINDUNGAN DATA PERIBADI (PENDAFTARAN PENGGUNA DATA) 2013 [*P.U. (A) 337/2013*]			
1.	Peraturan 5 Pembaharuan perakuan pendaftaran	Kegagalan untuk memperbaharui perakuan pendaftaran	Denda tidak melebihi RM250,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
2.	Peraturan 6 Perubahan butiran dalam perakuan pendaftaran	Kegagalan untuk memberitahu Pesuruhjaya Perlindungan Data Peribadi mengenai apa-apa perubahan kepada butiran dalam perakuan pendaftaran	Denda tidak melebihi RM250,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya
3.	Peraturan 8 Mempamerkan perakuan pendaftaran dan maklumat lain	Kegagalan untuk mempamerkan perakuan pendaftaran dan maklumat lain	Denda tidak melebihi RM10,000 atau dipenjarakan selama tempoh tidak melebihi satu (1) tahun atau kedua-duanya

GENERAL CODE OF PRACTICE OF PERSONAL DATA PROTECTION

ISSUED BY

Commissioner of Personal Data Protection Office

EFFECTIVE DATE

15th of December 2022

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

Ref.No.
CoP_Umum

IN exercise of the powers conferred by Section 24(1) of the Personal Data Protection Act 2010 [*Act 709*], I hereby register the General Code of Practice for the said Class of Data Users and it is applicable to all Data Users with immediate effect.

Dated : 15 December 2022

(MAZMALEK BIN MOHAMAD)
Personal Data Protection Commissioner, Malaysia

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

FOREWORD

This General Code of Practice of Personal Data Protection aims to enforce compliance to Section 23 of the Personal Data Protection Act [*Act 709*], regulations and standard and establish a guideline to the Class of Data Users who have not prepared a Code of Practice and there is no data user forum to develop the relevant Code of Practice for the Class of Data Users. Should you require further information, kindly consult —

The Personal Data Protection Commissioner at —
6th Floor, KKD Complex, Lot 4G9
Persiaran Perdana, Precint 4
Federal Government Administrative Centre
62100 Putrajaya Federal Territory
Malaysia
Tel: 03-89115000 Fax: 03-89117959
Email: info@pdp.gov.my

PRAKATA

Tataamalan Umum Perlindungan Data Peribadi ini bertujuan untuk menguatkuasakan pematuhan kepada Seksyen 23 Akta Perlindungan Data Peribadi 2010 [*Akta 709*], peraturan-peraturan dan standard serta mewujudkan garis panduan kepada Golongan Pengguna Data yang tidak menyediakan Tataamalan dan tidak ada forum pengguna data untuk membangunkan Tataamalan yang berkaitan. Sekiranya memerlukan maklumat lanjut, sila rujuk —

Pesuruhjaya Perlindungan Data Peribadi di —
Aras 6, Kompleks KKD, Lot 4G9
Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya, Malaysia
Tel: 03-8000 8000 | Faks: 03-8911 7959
E-mel: info@pdp.gov.my

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

1.1.1 Pursuant to the Appointment of Date of Coming into Operation [*P.U. (B) 464/2013*], the Personal Data Protection Act 2010 [*Act 709*] came into operation on 15 November 2013. Under Act 709, a body who has been designated by the Personal Data Protection Commissioner as a data user forum in respect of a specific Class of Data Users may prepare a Code of Practice (CoP).

1.1.2 Section 24 of Act 709 provides for instances where the Personal Data Protection Commissioner may issue CoP. This General CoP of Personal Data Protection shall apply to the Class of Data Users who have not prepared a CoP and there is no data user forum to develop the relevant CoP for the Class of Data Users.

1.1.3 The objective of this General CoP of Personal Data Protection is to set out best practices for the data user to assist him in meeting the requirements under Act 709 when undertaking commercial transactions. The examples provided in this General CoP of Personal Data Protection are not intended to be exhaustive but are included for context and for the purposes of illustration. The recommendations provided in this General CoP of Personal Data Protection are good practices and the data user is encouraged to adopt these practices.

1.1.4 This General CoP of Personal Data Protection shall be read together with Act 709, regulations, actions, orders, directions, notifications, approvals, decisions and other executive acts howsoever called, made, given or done by the Personal Data Protection Commissioner.

1.2 **Non-compliance with this General CoP of Personal Data Protection**

1.2.1 This General CoP of Personal Data Protection has the force of law and is effective once it is registered by the Personal Data Protection Commissioner. As this General CoP of Personal Data Protection is legally binding, any data user who fails to comply with any provision of this General CoP of Personal Data Protection that is applicable to the data user commits an offence, and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both under Section 29 of Act 709.

2. INTERPRETATION

For the purpose of this General CoP of Personal Data Protection, the various words and terms used throughout this General CoP of Personal Data Protection shall have the same meaning as per Act 709, unless specified otherwise.

Words	Meaning
personal data	means any information in respect of commercial transactions, which — (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject, but does not include any information that is processed for the purpose of a credit reporting business carried

	on by a credit reporting agency under the Credit Reporting Agencies Act 2010
sensitive personal data	means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other belief or a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the *Gazette*
vital interests	means matters relating to life, death or security of a data subject
use	in relation to personal data, does not include the act of collecting or disclosing such personal data
collect	in relation to personal data, means an act by which such personal data enters into or comes under the control of a data user
Minister	means the Minister charged with the responsibility for the protection of personal data
disclose	in relation to personal data, means an act by which such personal data is made available by a data user
relevant person	in relation to a data subject, howsoever described, means — (a) in the case of a data subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject; (b) in the case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the data subject to act on behalf of the data subject; or (c) in any other case, a person authorized in writing by the data subject to make a data access request, data correction request, or both such requests, on behalf of the data subject
direct marketing	means the communication by whatever means of any advertising or marketing material which is directed to particular individuals

correction	in relation to personal data, includes amendment, variation, modification or deletion
requestor	in relation to a data access request or data correction request, means the data subject or the relevant person on behalf on the data subject, who has made the request
data processor	in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes
processing	in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including — (a) the organization, adaptation or alteration of personal data; (b) the retrieval, consultation or use of personal data; (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of personal data
data user	means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of personal data, but does not include a data processor
relevant data user	in relation to — (a) an inspection, means the data user who uses the personal data system which is the subject of the inspection; (b) a complaint, means the data user specified in the complaint; (c) an investigation — (i) in the case of an investigation initiated by a complaint, means the data user specified in the complaint; (ii) in any other case, means the data user who is the subject of the investigation; (d) an enforcement notice, means the data user on whom the enforcement notice is served

third party	in relation to personal data, means any person other than — (a) a data subject; (b) a relevant person in relation to a data subject; (c) a data user; (d) a data processor; or (e) a person authorized in writing by the data user to process the personal data under the direct control of the data user
standard	means a minimum requirement issued by the Commissioner, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context
data subject	means an individual who is the subject of the personal data
commercial transactions	means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010

3. GENERAL PRINCIPLE (SECTION 6 OF ACT 709)

3.1 The General Principle provides that —

(a) the data user is required to obtain consent from the data subject prior to processing personal data unless the processing of personal data involves one of the following circumstances:

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

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

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

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

(v) for the administration of justice; or

(vi) for the exercise of any functions conferred on any person by or under the law; and

(b) for processing of sensitive personal data, the data user is required to obtain explicit consent of the data subject.

3.2 The processing of personal data including sensitive personal data can only be performed if —

(a) the data subject has given his consent;

(b) personal data is processed for a lawful purpose;

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

(d) personal data collected is adequate, relevant and not excessive to the purpose for which personal data is processed.

3.3 **Consent of the data subject**

3.3.1 The data user shall obtain consent from the data subject in relation to the processing of personal data in any form that such consent can be recorded and maintained properly by the data user.[1] If the form in which such consent is to be given also concerns another matter, the requirement to obtain consent shall be presented distinguishable in its appearance from such other matter.

3.3.2 Consent for collecting, processing and disclosing the data subject's personal data can be obtained in several ways. Such consent provides the clearest indication that the data subject has consented to notify purposes of the collection, processing or disclosure of his personal data.

[1] Subregulation 3(1) of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

3.3.3 Example of forms of consent —

(a) signature or clickable box indicating consent

☐ I hereby allow personal data processing rendered by me in this form for the purpose (s) _____ only. (state the purpose) Name: Identity Card Number: ***Example:*** *By clicking the "Agree" button through online application, it indicates that the data subject has provided consent for the processing of personal data.*

(b) consent by conduct or performance: consent is considered as given by way of conduct or performance if —

(i) the data subject does not object to the processing;

(ii) the data subject voluntarily discloses his personal data; or

(iii) the data subject proceeds to use the services of the data user; and

Example: *Consent is given by the data subject upon providing a copy of his identification document, whether or not it contains sensitive personal data to the data user.*

(c) verbal consent: may be recorded either digitally (such as through the use of call logger and/or recorder software) or by issuing a written communication (such as issuing a letter, a form or an email from the data user's official email) to the data subject confirming that consent has been given.

Example: *Consent is given by a caller to the data user to process the caller's personal data when the caller calls the data user's customer service for their services.*

3.3.4 The data user shall obtain consent from the parent, guardian or person who has parental responsibility on the data subject, if the data subject is under the age of eighteen (18) years.

3.3.5 The data user shall obtain consent from a person who is appointed by a court to manage the affairs of the data subject or a person authorized in writing by the data subject to act on his behalf if the data subject is incapable of managing his own affairs.

4. NOTICE AND CHOICE PRINCIPLE (SECTION 7 OF ACT 709)

4.1 The data user is required to make available a written notice, also known as a Personal Data Protection (PDP) Notice, to the data subject prior to or as soon as possible after the collection of his personal data. The PDP Notice is a written statement explaining how the data user processes personal data obtained from the data subject.

4.2 By examining the PDP Notice, the data subject should get a clear picture of how the data user will process personal data submitted and what options are available to the data subject. The PDP Notice should not be the platform for the data user to get the data subject's consent, especially a blanket consent. The data user has to obtain the consent in a proper method, to record and manage it accordingly.

4.3 **When to give the PDP Notice**

4.3.1 The PDP Notice shall be given as soon as practicable by the data user —

(a) when the data subject is first asked by the data user to provide his personal data;

(b) when the data user first collects the personal data of the data subject;

(c) before the data user uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or

(d) before the data user discloses the personal data to a third party.

4.4 **Compulsory Elements**

4.4.1 The PDP Notice shall contain the following elements:

(a) the processing of personal data
- To name the details of personal data involved.
- Type of personal data – to mention any sensitive personal data involved in processing.
- To mention if the personal data of children under 18 years old are processed.

(b) the need for processing
- The purpose of processing.
- To mention if there is any regulator requirement to collect certain personal data.
- How long the personal data will be retained in such processing.
- When will the personal data be disposed.

- What practical measures will be taken to ensure personal data is secured.

(c) the source of personal data

- To mention all the relevant internal and external sources which refer to from where the personal data is obtained (e.g.: manual or digital application/registration form).

(d) the rights of the data subject

- Personal data submission choice – compulsory or an option. If such personal data is compulsory, specify the consequences of not submitting it.
- How to access personal data submitted to the data user.
- How to correct or update the personal data.
- How to limit the processing of the personal data submitted - how to withdraw consent on personal data processing.
- How to contact data user for queries or complaints regarding personal data – to mention the name of person-in-charge, the designation, the contact number, and the e-mail address.

(e) the disclosure of personal data

- To name the third party to whom the personal data of data subject are shared with and for what purpose.
- To inform the security measures in place to ensure the disclosure implemented is safe and secure.

4.4.2 For the purposes of paragraph 7(1)*(d)* of Act 709, the data user shall provide the data subject the details as follows:

(a) designation of the contact person;

(b) phone number;

(c) fax number, if any;

(d) email address, if any; and

(e) such other related information.[2]

4.5 **Language**

4.5.1 The PDP Notice shall be in dual language; the national language and the English language. If there is any need to prepare the PDP Notice in other languages, the data user may do so.

4.6 **Method of Communication**

4.6.1 The data user may communicate the PDP Notice to the data subject by one or more of the following methods:

(a) posting a printed copy of the PDP Notice to the last known address of the data subject based on the data user's record;

(b) posting the PDP Notice on the website of the data user;

(c) issuing a short message service (SMS) to the data subject with a website address/link to the PDP Notice and/or a telephone number in order to request for the PDP Notice and/or further information;

(d) issuing an email to the data subject with a website address/link to the data user's PDP Notice and/or telephone number to contact for further information;

(e) issuing an electronic message to the data subject providing a website address/link to the data user's PDP Notice and/or

[2] Regulation 4 of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

telephone number to contact for further information via such other electronic channels utilised by the data user;

(f) inserting a summary notice in regular communications with the data subject (e.g. in monthly billing statements) with a website address/link to the PDP Notice and/or a telephone number to contact in order to request for the PDP Notice and/or further information;

(g) prominently displaying a summarised version of the PDP Notice at the premises of the data user's place of business (e.g. at the counter desk that the data subject comes to and/or at a prominent location in the data user's premises), and making available the full PDP Notice either upon a request being made at the counter to an employee of the data user;

(h) displaying a message on the screens of kiosks with a website address/link to the PDP Notice, a telephone number to contact for further information and/or stating that the PDP Notice is available at the branch of the data user;

(i) inserting a statement in application/registration forms referencing the PDP Notice, which may be accessed at a given website address/link, or by making a request to an employee of the data user, or by calling a telephone number provided in the application/registration form;

(j) printing out copies of the PDP Notice and providing it to the data subject at the data user's premises; or

(k) any other method of communication that serves to bring the PDP Notice to the data subject.

4.6.2 The data user shall determine the most appropriate method of communicating the PDP Notice which would reach as many of the data subjects as possible. It is recommended that the data user uses a variety of methods of communication to ensure that the PDP Notice is communicated as widely as possible.

4.6.3 The data user is required to maintain records of having communicated the PDP Notice to the data subject. This requirement may be fulfilled where the data user maintains evidence or records that the PDP Notice has been communicated to the data subject.

4.6.4 The data user may refer to a sample template of the PDP Notice issued by the Personal Data Protection Commissioner appended as **Appendix 1**.

5. DISCLOSURE PRINCIPLE (SECTION 8 OF ACT 709)

5.1 The disclosure of the data subject's personal data is limited to the purpose and related purposes for which the original consent was obtained under the Notice and Choice Principle. The purpose declared by the data user for the collection of personal data in the PDP Notice is of importance as it effects whether additional consent needs to be obtained under the Disclosure Principle. The Disclosure Principle is closely related to the Notice and Choice Principle.

5.2 No personal data shall, without the consent of the data subject, be disclosed for any purpose other than —

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

(b) a purpose directly related to the original purposes; or

(c) to any other party other than a third party of the class of third parties as specified in the PDP Notice.

5.3 Extent of further disclosure of personal data which falls outside the consent given by the data subject for the original purpose at the time collection is admissible. Such disclosure may be made under the following circumstances:[3]

(a) the data subject has given his consent to the disclosure;

(b) the disclosure —
(i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or
(ii) was required or authorized by or under any law or by the order of a court;

(c) the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;

(d) the data user acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or

(e) the disclosure was justified as being in the public interest in circumstances as determined by the Minister.

5.4 **List of disclosure**

5.4.1 The data user shall keep and maintain a list of disclosure to third parties for the purposes of paragraph 8*(b)* of Act 709 in relation to personal data of the subject data that has been or is being processed by him.[4]

[3] Section 39 Act 709
[4] Regulation 5 of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

5.5 **Disclosure to the data processor**

5.5.1 The data user is likely to disclose personal data to the data processor for various purposes relating to the data user's business. Where the data processor is engaged, it is recommended that the data user obtains warranties from the data processor in respect of the personal data to be disclosed. These warranties may include, among others —

(a) that the data user shall only process personal data for purposes relating to his appointment by the data user, in accordance with the data user's instructions, and no other purpose; and

(b) the data processor shall comply with all applicable laws, regulations and industry standards relating to the privacy, confidentiality or security of the personal data.

6. SECURITY PRINCIPLE (SECTION 9 OF ACT 709)

6.1 The data user 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 measure taken for ensuring the secure transfer of the personal data.[5]

6.2 The meaning of practical steps may vary from case to case, depending on the nature of personal data being processed by the data user and the degree of sensitivity attached to the personal data or the harm that the data subject might suffer due to its loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

6.3 **Establishment of the security standard for personal data processed electronically**

6.3.1 The data user shall, 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:[6]

DATA SECURITY FOR PERSONAL DATA PROCESSED ELECTRONICALLY	
No.	**Description**
1.	Register all employees involved in the processing of personal data.
2.	Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organization.
3.	Control and limit employee's access to personal data system for the purpose of collecting, processing and storing of personal data.
4.	Provide user ID and password for authorized employees to access personal data.
5.	Terminate user ID and password immediately when an employee who is authorized access to personal data is no longer handling the data.
6.	Establish physical security procedures as follows: i. control the movement in and out of the data storage site; ii. store personal data in an appropriate location which is

[5] Subsection 9(1) of Act 709
[6] Part II, No. 4, Personal Data Protection Standard 2015

	unexposed and safe from physical or natural threats; iii. provide a closed-circuit camera at the data storage site (if necessary); and iv. provide a twenty four (24) hours security monitoring (if necessary).
7.	Update the Back Up/Recovery System and anti-virus to prevent personal data intrusion and such.
8.	Safeguard the computer systems from malware threats to prevent attacks on personal data.
9.	The transfer of personal data through removable media device and cloud computing service is not permitted unless with written consent by an officer authorized by the top management of the data user's organization.
10.	Record any transfer of data through removable media device and cloud computing service.
11.	Personal data transfer through cloud computing service must comply with the personal data protection principles in Malaysia, as well as with personal data protection laws of other countries.
12.	Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Personal Data Protection Commissioner.
13.	Ensure that all employees involved in processing personal data always protect the confidentiality of the data subject's personal data.
14.	Bind an appointed third party by the data user with a contract for operating and carrying out personal data processing activities. This is to ensure the safety of personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

6.4 **Establishment of the security standard for personal data processed non-electronically**

6.4.1 The data user shall, 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:[7]

DATA SECURITY FOR PERSONAL DATA PROCESSED NON-ELECTRONICALLY	
No.	**Description**
1.	Register employees handling personal data into a system/registration book before being allowed access to personal data.
2.	Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organization.
3.	Control and limit employee's access to personal data system for the purpose of collecting, processing and storing of personal data.
4.	Establish physical security procedures as follows: i. store all personal data orderly in files; ii. store all files containing personal data in a locked place; iii. keep all the related keys in a safe place; iv. provide record for keys storage; and v. store personal data in an appropriate location which is unexposed and safe from physical or natural threats.
5.	Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Personal Data Protection Commissioner.
6.	Ensure that all employees involved in processing personal data always protect the confidentiality of the data subject's personal data.
7.	Record personal data transferred conventionally such as through mail, delivery, fax and etc.
8.	Ensure that all used papers, printed documents or other documents

[7] Part II, No. 5, Personal Data Protection Standard 2015

	exhibiting personal data are destroyed thoroughly and efficiently by using shredding machine or other appropriate methods.
9.	Conduct awareness programmes to all employees (if necessary) on the responsibility to protect personal data.

6.5 The data user shall ensure that the security standard in the processing of personal data be complied with by any data processor that carries out the processing of the personal data on behalf of the data user.[8] Where processing of personal data is carried out by the data processor on behalf of the data user, it is recommended that the data user uses reasonable efforts to include in his agreement with the data processor (whether in form of a contract, letter or any formal written document) —

(a) provision on confidentiality, non-disclosure and technical and/or organizational security measures;

(b) conditions under which personal data may be processed;

(c) representations, undertakings, warranties and/or indemnities which are to be provided by the data processor;

(d) security measures governing the processing to be carried out as may reasonably be contained in the data user's internal security policy and/or standards; and

(e) deletion, destruction and/or return of personal data that is under the control of the data processor upon completion or termination of the contract or engagement, unless the user decides otherwise.

Example: *Security measures or controls should be implemented for high risk processing activities, may include but not limited to Robot Process Automation (RPA), artificial intelligence, data analysis and prospective emerging technologies.*

[8] Subregulation 6(3) of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

7. RETENTION PRINCIPLE (SECTION 10 OF ACT 709)

7.1 The Retention Principle restricts the data user from keeping personal data processed for any purpose longer than necessary for the fulfilment of the purpose. The data user may retain, keep or hold personal data of the data subject for as long as it is necessary to fulfil the purpose for which it was collected and in relation to the data user's business requirements provided that the retention is done according to the relevant legal and statutory requirements.

7.2 The provisions of other specific legislation concerning retention of personal data shall not be affected by the retention principle of Act 709 and such other applicable legislation shall be read together.

7.3 **The standard for retention of personal data which is processed electronically and non-electronically**

7.3.1 The data user shall 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 by having regard[9] —

No.	Description
1.	Determine the retention period in all legislation relating to the processing and retention of personal data are fulfilled before destroying the data.
2.	Keep personal data no longer than necessary unless there are requirements by other legal provisions.
3.	Maintain a proper record of personal data disposal periodically and make such record available for submission when directed by the Personal Data Protection Commissioner.
4.	Dispose personal data collection forms used in commercial transactions within the period not exceeding fourteen (14) days, except if/unless the forms carry legal values in relation to the commercial transactions.
5.	Review and dispose all unwanted personal data that in the database.

[9] Part II, No. 6, Personal Data Protection Standard 2015

6.	Prepare a personal data disposal schedule for inactive data with a twenty four (24) months period. The personal data disposal schedule should be maintained properly.
7.	The use of removable media device for storing personal data is not permitted without written approval from the top management of the organization.

7.4 **Disposal of personal data**

7.4.1 It shall be the duty of the data user 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.[10]

7.4.2 Destruction is applicable to the paper based personal data and permanent deletion is applicable to the electronic personal data.

7.4.3 For personal data stored on an electronic medium, the permanent deletion of the personal data requires the electronic media (such as hard drive or a removable media device) to be wiped clean once the personal data has been deleted. The data user is to take reasonable effort to permanently delete the personal data from electronic media.

7.4.4 In the event of disposal, a disposal record should be kept to evidence the act of the disposal, *i.e.* by way of logbook, photographs or other methods that is relevant for record of disposal.

8. DATA INTEGRITY PRINCIPLE (SECTION 11 OF ACT 709)

8.1 **Establishment of data integrity standard for personal data processed electronically and non-electronically**

8.1.1 The data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having

[10] Subsection 10(2) of Act 709

regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed. Such measures are:[11]

No.	Description
1.	Provide personal data update form for data subjects, either via online or conventional.
2.	Update personal data immediately once data correction notice is received from data subject.
3.	Ensure that all relevant legislation is fulfilled in determining the type of documents required to support the validity of the data subject's personal data.
4.	Notify on personal data updates either through the portal or notice at premises or by other appropriate methods.

8.2 What amounts to reasonable steps may differ from case to case, depending on the circumstances of each case as well as on the purpose and directly related purposes that the personal data was obtained for.

8.3 By way of illustration, Act 709 requires the data user to take reasonable steps to ensure that the personal data processed in relation to the data subject is —

(a) accurate – meaning that the personal data is captured correctly;

(b) complete – meaning that information in relation to the data subject has not been omitted;

(c) not misleading – meaning that the personal data processed should not be ambiguous, deceiving or an oversight; and

(d) kept up-to-date – meaning that the personal data of the data subject should reflect the latest verified information in respect of the data subject.

[11] Part II, No. 6, Personal Data Protection Standard 2015

9. ACCESS PRINCIPLE (SECTION 12 OF ACT 709)

9.1 Access Principle requires the data user to give the data subject the right to access and correct his personal data which is inaccurate, incomplete, misleading or not up-to-date except where compliance with a request to such access or correction is refused under Act 709.

9.2 Compliance to the Access Principle

9.2.1 In complying with the Access Principle, the data user shall observe the data subject's right to access the personal data and the right to correct the personal data in accordance with Act 709. The data user may refuse the right of the data subject to access and/or to correct his personal data provided that the refusal is in accordance with Act 709.

9.3 The maximum fees payable for a data access request by the data subject, as provided by the Personal Data Protection (Fees) Regulations 2013 [*P.U. (A) 338/2013*] are specified below[12] —

Item	Description	Maximum fee (RM)
1.	Data access request for a data subject's personal data with a copy	10
2.	Data access request for a data subject's personal data without a copy	2
3.	Data access request for a data subject's for a data subject's sensitive personal data with a copy	30
4.	Data access request for a data subject's sensitive personal data without a copy	5

[12] First Schedule, Regulation 2, Maximum Fees for Data Access Request, Personal Data Protection (Fees) Regulations 2013 [*P.U. (A) 338/2013*]

10. RIGHTS OF THE DATA SUBJECT

10.1 Act 709 provides the data subject with the following rights:

(a) right of access to personal data;

(b) right to correct personal data;

(c) right to withdraw consent to process personal data;

(d) right to prevent processing likely to cause damage or distress; and

(e) right to prevent processing for purposes of direct marketing.

10.2 **Right of access to personal data**

10.2.1 The data subject is entitled to access his personal data which is being processed by or on behalf of the data user and has the right to lodge a Data Access Request ("DAR") with the data user and to receive a reply from the data user within the time period provided in Act 709. For avoidance of doubt, personal data being retained for back up is not subject to be accessed by the data subject.

10.2.2 It is recommended that the data user provides a DAR form at suitable places and easy to obtain at the premises of the data user's place of business when required by the data subject at the time of request. The data user may refer to a sample template of the DAR Form appended as **Appendix 2**.

10.2.3 **Compliance by the data user with the DAR**

The data user shall comply with the DAR by —

(a) ensuring payment of the prescribed fees in accordance with the First Schedule of the Personal Data Protection (Fees) Regulations

2013 [*P.U. (A) 338/2013*] is made by the data subject. It is advised that the fees payable for the submission of the DAR to be stated in the DAR Form;

(b) providing a standard form for request to access the personal data by the requestor;

(c) providing the requestor a copy of the personal data of the data subject in any form as long as it can be comprehended by the requestor within twenty one (21) days from the date of receipt of the DAR;

(d) if the data user is not able to comply with the DAR within the twenty (21) days' period, the data user is required to notify the requestor by notice in writing as to the reasons of his inability to do so and thereafter to comply with the valid DAR to the extent he is able to do so; and

(e) complying in whole with the DAR not later than fourteen (14) days after the expiration of the twenty one (21) days' period.

10.2.4 **Refusal by the data user to comply with the DAR**

The data user has the right to refuse to comply with the DAR if —

(a) inability to verify identity. The data user is not provided with necessary information as the data user may reasonable require in order to establish the identity of the data subject or where the DAR is submitted by the requestor, establish the requestor's connection to the data subject;

(b) the data user is not provided with sufficient information to locate the personal data to which the data access request relates;

(c) disproportionate burden. The burden or expense of providing access to personal data is disproportionate to the risk to the data subject's privacy for example if the time and cost to be incurred by the data user is greater than the significance of the personal data requested under the DAR;

(d) disclosure of another. The data user is unable to comply with the DAR without disclosing another data subject's personal data. In such a situation, the data user may either anonymise other data subject's personal data or seek consent from the data subject, or by any other practical means to disclose the personal data without breaching Act 709;

(e) providing access would constitute a violation of an order of a court;

(f) providing access would disclose confidential commercial information; or

(g) such access to personal data is regulated by another law.

10.3 **Right to correct personal data**

10.3.1 The data subject is entitled to request personal data held by the data user be corrected if he is satisfied that the personal data is inaccurate, incomplete, misleading or not up-to-date by submitting a Data Correction Request ("DCR").

10.3.2 It is recommended that the data user provides a DCR Form at suitable places and easy to obtain at the premises of the data user's place of business when required by the data subject at the time of request. The data user may refer to a template of the DCR Form appended as **Appendix 3**.

10.3.3 **Validity of the DCR**

In ensuring that the DCR is valid, the data user is required to ensure that —

(a) the DCR is made in writing;

(b) the DCR is specific as to the personal data to be corrected;

(c) the DCR contains the necessary information with certified documentation to establish the identity of the requestor and if the requestor is not the data subject, to establish the right and identity of the requestor and relationship of the requestor with the data subject;

(d) the data user is supplied with such information as he may reasonably acquire to ascertain in what way the personal data to which the data correction relates is inaccurate, incomplete, misleading or not up-to-date;

(e) the data user is satisfied that the personal data to which the data correction relates is inaccurate, incomplete, misleading or not up-to-date; and

(f) the data user controls the processing of the personal data to which the data correction request relates and is not prohibited by another data user from complying with the data correction request.

10.3.4 **Compliance by the data user with the DCR**

The data user shall comply with the DCR not later than twenty one (21) days from the date of receipt of the DCR by —

(a) making the necessary correction to the personal data;

(b) supplying the requestor with a copy of the personal data as corrected;

(c) taking all practicable steps to supply the third party with a copy of the corrected personal data accompanied by a notice in writing stating the reasons for the correction;

(d) if the data user is unable to comply with a valid DCR within the twenty one (21) days' period from the date of receipt of the DCR, shall before the expiration of that period —

(i) inform the requestor by notice in writing that he is unable to comply with the DCR within such period and the reasons why he is unable to do so; and

(ii) comply with the DCR to the extent that he is able to do so; and

(e) complying in whole with the DCR not later than fourteen (14) days after the expiration of the twenty one (21) days' period.

10.3.5 **Refusal by the data user to comply with the DCR**

The data user has the right to refuse to comply with the DCR if —

(a) inability to verify identity. The data user is not provided with necessary information as the data user may reasonable require in order to establish the identity of the data subject or where the DCR is submitted by the requestor, establish the requestor's connection to the data subject;

(b) inability to verify the need for correction. The data user is not supplied with sufficient information as the data user may reasonably require to determine how the personal data is inaccurate, incomplete, misleading or not up-to-date;

(c) the data user is not satisfied that the personal data to which the DCR relates is inaccurate, incomplete, misleading or not up-to-date; or

(d) the data user is not satisfied that the correction requested is accurate, complete, not misleading or up-to-date.

10.4 **Right to withdraw consent to the processing of personal data**

10.4.1 The data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject.[13]

10.4.2 The data user shall, upon receiving the notice cease the processing of the personal data except to the extent where the withdrawal of consent would affect the data user's rights and obligations under contract or law. Example of such rights and obligations include —

(a) the right to be paid for the services rendered, for example, the settlement of bookings or tax invoices or overdue payments;

(b) the right to bring and maintain legal proceedings against the data subject;

(c) the right to commence or continue with internal investigations involving the data subject;

(d) the obligation to maintain personal data for such durations as required under applicable legislation; and

(e) the conduct of internal audits, risk management and/or fulfilment of legal or regulatory reporting requirements.

[13] Subsection 38(1) of Act 709

10.5 **Right to prevent processing likely to cause damage or distress**

10.5.1 The data subject may, at any time by notice in writing to the data user, require the data user to —

(a) cease processing the personal data; or

(b) not begin the personal data processing,

where the processing is causing or is likely to cause substantial and unwarranted damage or distress to the data subject or another person.

10.5.2 **Requirement**

The data subject is required to prove that —

(a) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person; and

(b) the damage or distress is or would be unwarranted.

In most cases —

(a) "substantial damage" includes financial loss suffered by the data subject or another person;

(b) "substantial distress" includes emotional or mental trauma suffered by the data subject or another person; and

(c) "unwarranted" means that the damage or distress suffered by the data subject or another person is not justifiable.

10.5.3 **Circumstances where the data subject does not have the right to prevent processing**

The data subject shall not have the right to prevent processing where —

(a) the data subject has consented to the processing; or

(b) the processing of personal data is necessary —
  (i) for the performance of a contract to which the data subject is a party;
  (ii) for the taking of steps at the request of the data subject with a view to entering into a contract;
  (iii) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by contract; or
  (iv) in order to protect the vital interests of the data subject.

10.5.4 **Compliance by the data user with the right to prevent processing likely to cause damage or distress**

Upon receiving a written notice to cease processing or not to commence processing of personal data, the data user shall, within twenty one (21) days, provide the data subject a written notice stating —

(a) that the data user has complied or intends to comply with the data subject notice;

(b) if the data user does not intend to comply with the data subject notice, to provide reasons for the decision; or

(c) stating reasons why the data user finds the data subject notice unjustified or to any extent unjustified and the extent to which the data user has complied or intends to comply (if any).

The data user may consider the following when making a decision on whether to comply with the request —

(a) are there legitimate reasons for the data subject's request? The data subject should provide legitimate reasons as the damage or distress caused shall be substantial; and

(b) is the damage or distress unwarranted? This is tied to whether the data subject has provided legitimate reasons for the request.

Where the data user does not comply with the notice, the data subject may apply to the Personal Data Protection Commissioner to require the data user to comply with the notice. If the Personal Data Protection Commissioner is satisfied that the data subject's request is justified, the Personal Data Protection Commissioner may require the data user to comply with the request.

10.6 **Right to Prevent Processing for Purposes of Direct Marketing**

10.6.1 Pursuant to Act 709, the data subject has the right at any time, by notice in writing to the data user, to require the data user to either cease or not begin processing his personal data for purposes of direct marketing. The data user may refer to a sample template of the notice under Subsection 43(1) of Act 709 appended as **Appendix 4**.

10.6.2 The data user shall comply with such a request within a reasonable time frame.

10.6.3 The data user who is communicating advertising or marketing materials directed to a particular data subject, through the utilisation of the data subject's personal data, is required to either has already notified the data subject via his PDP Notice, or in cases where the PDP Notice is silent as to the issuance of

such advertising or marketing materials, is required to obtain the consent of the data subject prior to commencing direct marketing.

10.6.4 The data user is permitted to conduct direct marketing to the data subject —

(a) if consent is obtained from the data subject;

(b) for the collection of personal data for sale of products or provision of services;

(c) if the data subject is informed of the identity of direct marketing organisations and the purpose of collection and disclosure;

(d) in the event the product and/or services offered to the data subject are similar to the product and services generally provided by the data user; or

(e) in the event the data user is committed to providing an opt-out option for the data subject during the collection of personal data.

10.6.5 Where the data subject makes a written request asking to receive some direct marketing materials and not others, the data user may choose not to provide the data subject with all direct marketing materials, should his system be incapable of distinguishing between the different types of direct marketing materials.

10.6.6 If the data subject is dissatisfied with the failure of the data user to comply in whole or in part with the written request, the data subject may submit an application to the Personal Data Protection Commissioner to require the data user to comply. Failure by the data user to comply with the requirement of the Personal Data Protection Commissioner constitutes an offence liable to

punishment with a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two (2) years or to both.[14]

11. GENERAL CoP OF PERSONAL DATA PROTECTION COMPLIANCE AND MONITORING

11.1 The data user is required to maintain a personal data system. The personal data system shall at all reasonable times be open to the inspection of the Personal Data Protection Commissioner or any inspection officer.[15]

11.2 The data user shall maintain —

(a) in relation to the General Principle, the record of the consent from the data subject maintained in respect of the processing of personal data by the data user;

(b) in relation to the Notice and Choice Principle, the record of a written notice issued by the data user to the data subject in accordance with Section 7 of Act 709;

(c) in relation to the Disclosure Principle, the list of disclosure to third parties for the purposes of paragraph 8*(b)* of Act 709 in respect of personal data that has been or is being processed by him;

(d) in relation to the Security Principle, the security policy developed and implemented by the data user for the purposes of Section 9 of Act 709;

(e) in relation to the Retention Principle, the record of compliance in accordance with the retention standard;

(f) in relation to the Data Integrity Principle, the record of compliance in accordance with the data integrity standard; or

(g) such other related information which the Personal Data Protection Commissioner or any inspection officer deems necessary.

[14] Subsection 42(6) of Act 709
[15] Subregulation 14(1) of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

11.3 The data user is required to develop and implement appropriate compliance policies and procedures (compliance framework) in order to ensure compliance with this General CoP of Personal Data Protection, Act 709, regulations and standard.

11.4 It is recommended that the data user continuously monitor his compliance with this General CoP of Personal Data Protection, Act 709, regulations and standard by —

(a) implementing an internal monitoring framework; and

(b) conducting self-audits.

11.5 The data user is encouraged to ensure that appropriate training and/or awareness is put in place for employees to ensure that employees understand the importance of complying with these policies and procedures. Relevant employees may be identified to receive specific training, such as training on security and fraud awareness and on handling data access/correction requests.

11.6 The data user is required to ensure that he keeps up with the latest developments in Act 709 and continue to provide training to employees as and when required to keep up with any changes.

12. REQUIREMENT OF PREPARING A COP FOR THE SPECIFIC CLASS OF DATA USERS

12.1 A body who has been designated by the Personal Data Protection Commissioner as a data user forum in respect of a specific class of data shall prepare a CoP for the specific class of data users within two (2) years from the date of the designation.

12.2 The Personal Data Protection Commissioner may revoke, amend or revise, whether in whole or in part, any CoP registered under Act 709 by virtue of Section 26 of Act 709.

Appendix 1

Personal Data Protection Notice

[Logo / Organisation name]

(Effective date: dd mm yy)
(Last reviewed: dd mm yy)

INTRODUCTION

(Insert organisation name) care about your personal data protection. This notice clarifies how (your business name) processes your data from the point we collect, use, share, dispose of and the security measures that we established to ensure your personal data is well protected.

COLLECTION OF PERSONAL DATA

We collect your personal data which range from your name, home address, email address, phone number and your bank account. [Change / add to this list as appropriate]

SOURCE OF PERSONAL DATA COLLECTION

We gather your personal data from:

1. New member registration form available at our website (your website address)
2. Purchase form
3. Cookies
4. [Change / add to this list as appropriate]

REASON FOR PERSONAL DATA COLLECTION

We collect your personal data to:

1. Process your request to purchase our product / service
2. Deliver our product to your desired address and location
3. Resolve complaint / delivery problem (if any)
4. Send new product promotion to you (only with your consent)
5. [Change / add to this list as appropriate]

PROCESSING OF PERSONAL DATA

We only process your personal data within Malaysia. Your personal data will not be transferred to any place outside Malaysia. [Change as appropriate]

DISCLOSURE OF PERSONAL DATA

We disclose your personal data to:

1. The appointed courier to deliver your purchased product
2. The authority for legal / regulatory purpose (name the parties involved)
3. [Change / add to this list as appropriate]

SECURITY MEASURE

We take these measures to protect your personal data:

1. By ensuring your personal data is kept as required by Act 709
2. By ensuring our staff not to misuse your personal data
3. By performing contract / agreement with system vendor, appointed courier company.
4. [Change / add to this list as appropriate]

Nevertheless, you are required to ensure the security of your password and not to disclose it to another party to reduce the risk of data breaches.

PERSONAL DATA RETENTION PERIOD

We will retain your personal data for seven (7) years / as long as you are our customer [Change as appropriate]. If you are no longer our customer, we will permanently delete your personal data.

YOUR RIGHTS

You have the rights to:

1. Correct / update your personal data (insert the link to the form available)
2. Access your personal data which we process and keep with us
3. Stop any of our new promotional products sent to you
4. Withdraw your consent for us to process your personal data [Inform the consequences].

CONTACT US

You can contact us or submit your inquiry in regards to the processing of your personal data at:

(Name)

(Designation)

(Address)

(Telephone number)

(Fax number / email address)

Appendix 2

PERSONAL DATA PROTECTION ACT 2010 [*ACT 709*]
PERSONAL DATA ACCESS REQUEST FORM

The following information is required to help us provide you a timely and accurate response to your Personal Data Access Request pursuant to Act 709.

Full Name of Data Subject or Relevant Person	
Relevant Person's Relationship with the Data Subject	
Address	
Mobile Number	
Email address	
Please provide details of the information you require from [Data User]:	

Declaration: I am the Data Subject/Relevant Person named above and hereby request, under the provisions of Sections 12 and 30 of the Personal Data Protection Act 2010 [*Act 709*], that [**Data User**] provide me with a copy of the personal data held about me as specified above. I understand that there may be a charge for this service and that [**Data User**] will contact me to request payment. I also note that the [**Data User**] will respond within the time stipulated under Act 709 after receipt of payment from me and will notify me of a date and time to collect a copy of the documents personally.

Signature …… Date ……

Appendix 3

PERSONAL DATA CORRECTION REQUEST FORM	
• Please note that we reserve the right to restrict and/ or refuse your access to certain particulars of your personal data as may be permitted under the Personal Data Protection Act 2010 [*Act 709*]. • Your request may not be processed if the information/document provided is incomplete. • Any request for Personal Data Correction Request must be supported with proof or evidence. • Please use CAPITAL LETTERS to fill in the form.	
Please tick (√) on one of the following: ☐ I would like to access my personal data (Please fill in Section 1 and Section 3 below) ☐ I am a Third Party Requestor (Please fill in Section 2 and Section 3 below)	
SECTION 1 : TO BE FILLED IN BY DATA SUBJECT	
Full Name (per NRIC/Passport)	
New NRIC/Passport No.	
Mobile Phone No.	
SECTION 2: TO BE FILLED IN BY THIRD PARTY REQUESTOR (AUTHORIZED PERSON) This request is based on (please tick (√) one of the following): ☐ I am acting under the Data Subject's authorisation/mandate/Power of Attorney ☐ I am the legal/personal representative of the Data Subject ☐ I have Warrant or Court Order allowing the correction to the Data Subject's Personal Data ☐ I am executor/administrator of the Data Subject's estate ☐ Others (please specify) _____ Please enclose proof of your authority to correct the personal data of the Data subject.	

A : Particulars of Data Subject	
Full Name (per NRIC/Passport)	
New NRIC/Passport No.	
Mobile Phone	
B: Particulars of Third Party Requestor	
Full Name (per NRIC/Passport)	
New NRIC/Passport No.	
Mobile Phone	
Email Address	
Correspondence Address	

SECTION 3 : CORRECTION OF PERSONAL DATA (Please tick (√) and fill in at relevant Section only)	
□ Full Name (per NRIC/Passport)	
□ New NRIC/Passport No.	
□ Address of premise	
□ Mobile Phone	
□ Postal Address	
□ *House Phone No.	
□ *Office Phone No.	
**Non-mandatory information*	

DECLARATION	
Declaration by the Data Subject I,…… declare that I am the person named in Section 1 and I am requesting to correct my own personal data. I confirm that the information supplied in this form is true and accurate. Signature: ..... Date: ……..	**Declaration by the Third Party Requestor** I,…… declare that I am the Authorized Person named in Section 2 and I am requesting to correct the Data Subject's personal data. I confirm that the information supplied in this form is true and accurate. Signature: …… Date: …….

FOR OFFICE USE ONLY (Please fill in relevant section only)	
□ APPROVED DATE UPDATED: ATTENDED BY:	□ NOT APPROVED REASON: NOTIFICATION DATE: ATTENDED BY:

Appendix 4

NOTICE UNDER SUBSECTION 43(1) OF

THE PERSONAL DATA PROTECTION ACT 2010 [*ACT 709*]

Date:

Data User's Address:

..……

..……

..……

Sir / Madam,

NOTICE UNDER SUBSECTION 43(1) OF THE PERSONAL DATA PROTECTION ACT 2010 [*ACT 709*] TO PREVENT PROCESSING OF PERSONAL DATA FOR PURPOSES OF DIRECT MARKETING

I, …… (full name) …… (New NRIC/Passport No.) need you to cease or not to begin processing my personal data for purposes of direct marketing in the duration of _____ * from the date of receipt of this notice.

Thank you.

Signature: ..……

Name: ..……

Address: ..……

..……

..……

..……

Phone No.: ..……..

Email: ..…….

*Data subject can determine a reasonable stipulated time

Appendix 5

LIST OF OFFENCES AND PUNISHMENTS UNDER THE PERSONAL DATA PROTECTION ACT 2010 [*ACT 709*] AND SUBSIDIARY LEGISLATION

ITEM	SECTION / REGULATION	OFFENCE	PUNISHMENT
1.	Subsection 5(2) Personal Data Protection Principles	Non-compliance with data processing under the Personal Data Protection Principles	Fine not exceeding RM300,000 or imprisonment for a term not exceeding two (2) years or both
2.	Subsection 16(4) Certificate of registration	Process personal data without certificate of registration issued in paragraph 16(1)*(a)*	Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both
3.	Subsection 18(4) Revocation of registration	Process personal data after registration is revoked	Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both
4.	Subsection 19(2) Surrender of certificate of registration	Failure to surrender the certificate of registration to the Personal Data Protection Commissioner after it is revoked	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both
5.	Section 29 Non-compliance with the CoP	Non-compliance with any provision of the CoP that is applicable to the data user	Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both
6.	Subsection 37(4) Notification of refusal to comply with data correction request	Non-compliance with any provision in subsection 37(2)	Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both
7.	Subsection 38(4)	Continue to process	Fine not exceeding

	Withdrawal of consent to process personal data	personal data after withdrawal of consent by the data subject	RM100,000 or imprisonment for a term not exceeding one (1) year or both
8.	Subsection 40(3) Processing of sensitive personal data	Processing sensitive personal data without complying with the conditions in subsection 40(1)	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both
9.	Subsection 42(6) Right to prevent processing likely to cause damage or distress	Non-compliance with the Personal Data Protection Commissioner's requirements in subsection 42(5)	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both
10.	Subsection 43(4) Right to prevent processing for purposes of direct marketing	Non-compliance with the Personal Data Protection Commissioner's requirements in subsection 43(3)	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both
11.	Subsection 108(8) Enforcement notice	Non-compliance with an enforcement notice	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both
12.	Subsection 113(7) Search and seizure with warrant	A person who without lawful authority, breaks, tampers with or damages the seal referred to in subsection 113(6) or removes any computer, book, account, computerised data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under seal or attempts to do so	Fine not exceeding RM50,000 or imprisonment for a term not exceeding six (6) months or both

13.	Section 120 Obstruction to search	Any person who — (a) refuses to give access to any authorized officer; (b) assaults, obstructs, hinders or delays any authorized officer; or (c) refuses any authorized officer any information relating to an offence or suspected offence	Imprisonment for a term not exceeding two (2) years or fine not exceeding RM10,000 or both
14.	Subsection 129(5) Transfer of personal data to places outside Malaysia	Non-compliance with requirements in subsection 129(1) — transfer personal data of a data subject to a place outside Malaysia unless to such a place as specified by the Minister, upon the recommendation of Personal Data Protection Commissioner, by notification published in the *Gazette*	Fine not exceeding RM300,000 or imprisonment for a term not exceeding two (2) years or both
15.	Subsection 130(7) Unlawful collecting, etc., of personal data	Committing offences as prescribed in section 130	Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both
16.	Subsection 131(1) and (2) Abetment and attempt punishable as offences	Subsection 131(1) Abetment of a commission of or attempts to commit any offence under Act 709	Provided that any term of imprisonment shall not exceed half of the maximum term provided for the offence under Act 709

		Subsection 131(2) Commission of any act preparatory to or in furtherance of the commission of any offence under Act 709	Provided that any term of imprisonment shall not exceed half of the maximum term provided for the offence under Act 709
17.	Subsection 141(2) Obligation of secrecy	Offence under paragraphs 141(1)*(a)* and *(b)* — the Personal Data Protection Commissioner, its officer or servant, any member of the Advisory Committee, any member, officer or servant of the Appeal Tribunal, any authorized officer or any person attending any meeting or deliberation of the Advisory Committee, whether during or after his tenure of office or employment, at any time shall not disclose any information obtained by him in the course of his duties	Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both
18.	Subsection 143(3) Power to make regulation	Non-compliance with any regulation or any other subsidiary legislation under this section	Fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both
PERSONAL DATA PROTECTION REGULATIONS 2013 [*P.U. (A) 335/2013*]			
1.	Regulation 12 Penalty	Non-compliance with the following:	Fine not exceeding RM250,000 or imprisonment

		• subregulation 3(1) consent of data subject • regulation 6 security policy • regulation 7 retention standard • regulation 8 • data integrity standard	for a term not exceeding two (2) years or both
PERSONAL DATA PROTECTION (REGISTRATION OF DATA USER) REGULATIONS 2013 [*P.U. (A) 337/2013*]			
1.	Regulation 5 Renewal of certificate of registration	Failure to renew certificate of registration	Fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both
2.	Regulation 6 Change of particulars in certificate of registration	Failure to notify the commissioner of any change to the particulars of certificate of registration	Fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both
3.	Regulation 8 Display of certificate of registration and other information	Failure to display certificate of registration and other information	Fine not exceeding RM10,000 or imprisonment for a term not exceeding one (1) year or both