KEMENTERIAN DIGITAL

GARIS PANDUAN
PERLINDUNGAN DATA PERIBADI

PEMINDAHAN DATA PERIBADI RENTAS SEMPADAN (CBPDT)

Versi 1.0

Tarikh Terbitan: 29 April 2025

PESURUHJAYA PERLINDUNGAN DATA PERIBADI MALAYSIA

Alamat:

PESURUHJAYA PERLINDUNGAN DATA PERIBADI MALAYSIA

Aras 8, Galeria PjH, Jalan P4W, Persiaran Perdana

Presint 4, Pusat Pentadbiran Kerajaan Persekutuan

62100 Putrajaya, Malaysia

ISI KANDUNGAN

BAHAGIAN A: PENGENALAN

1. Latar Belakang

1.1 Seksyen 129 Akta Perlindungan Data Peribadi 2010 [Akta 709] ("**Akta 709**") mengawal selia pemindahan data peribadi ke luar Malaysia. Bagi melaksanakan pemindahan data peribadi rentas sempadan, pengawal data dikehendaki mematuhi peruntukan di bawah Seksyen 129 Akta 709.

1.2 Garis Panduan ini ditetapkan sebagai panduan untuk menjelaskan keperluan-keperluan pematuhan dengan setiap syarat yang dinyatakan di bawah Seksyen 129 Akta 709 dan untuk membantu pengawal data dalam memutuskan syarat yang boleh dirujuk untuk sebarang pemindahan data peribadi rentas sempadan.

1.3 Sila ambil perhatian bahawa contoh-contoh yang diberikan dalam Garis Panduan ini tidak bertujuan untuk menjadi menyeluruh dan hanya disertakan untuk konteks dan tujuan ilustrasi.

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

2. Peruntukan Undang-Undang

2.1 Garis Panduan ini dikeluarkan oleh Pesuruhjaya menurut subseksyen 48(g) Akta 709.

3. Tafsiran

3.1 Melainkan jika ditakrifkan sebaliknya dalam Garis Panduan ini, istilah-istilah dan pernyataan-pernyataan yang digunakan di sini hendaklah mempunyai makna yang sama seperti yang diberikan di bawah Akta 709 dan mana-mana instrumen perundangan lain yang berkaitan di bawah Akta 709.

3.2 Dalam Garis Panduan ini, melainkan konteksnya memerlukan sebaliknya:

"**Notis perlindungan data peribadi**"	ertinya notis bertulis yang dihendaki diberikan oleh pengawal data kepada subjek data selaras dengan Seksyen 7 Akta 709;
"Penerima"	ertinya pengawal data dan/ atau pemproses data yang menerima data peribadi subjek data di luar Malaysia;
"**Penilaian Impak Pemindahan**"	ertinya merupakan penilaian risiko yang dijalankan untuk menilai rangka kerja perundangan dan kawal selia di negara/ bidang kuasa penerima data peribadi, bagi memastikan negara/wilayah berdaulat penerima mempunyai undang-undang yang sebahagian besarnya serupa dengan Akta 709 atau tahap perlindungan yang mencukupi bagi pemprosesan data peribadi;
"**Sijil Diiktiraf**"	ertinya sijil yang dikeluarkan oleh badan bertauliah atau pihak berkuasa yang mengesahkan bahawa pengawal data atau pemproses data mematuhi standard atau undang-undang perlindungan data sama ada di peringkat tempatan atau antarabangsa.

BAHAGIAN B: SYARAT BAGI PEMINDAHAN DATA PERIBADI KE TEMPAT DI LUAR MALAYSIA

4. Syarat-syarat bagi pemindahan data peribadi rentas sempadan

4.1 Subseksyen 129(2) Akta 709 memperuntukkan bahawa pengawal data boleh memindahkan sebarang data peribadi seorang subjek data ke mana-mana tempat di luar Malaysia jika:

(a) di tempat itu ada berkuat kuasa mana-mana undang-undang yang sebahagian besarnya serupa dengan Akta 709; atau

(b) tempat itu memastikan suatu tahap perlindungan yang mencukupi berhubung dengan pemprosesan data peribadi yang sekurang-kurangnya setara dengan tahap perlindungan yang diberikan oleh Akta 709.

4.2 Walau apa pun subseksyen 129(2) Akta 709, pengawal data boleh memindahkan mana-mana data peribadi ke suatu tempat di luar Malaysia jika:

4.2.1 subjek data telah memberikan persetujuan untuk pemindahan tersebut;

4.2.2 pemindahan itu perlu bagi pelaksanaan suatu kontrak antara subjek data dan pengawal data;

4.2.3 pemindahan itu perlu bagi penyempurnaan atau pelaksanaan suatu kontrak antara pengawal data dengan pihak ketiga yang —

(a) dibuat atas permintaan subjek data; atau

(b) adalah untuk kepentingan subjek data;

4.2.4 pemindahan itu adalah untuk tujuan prosiding undang-undang atau bagi tujuan mendapatkan nasihat undang-undang atau untuk mewujudkan, menjalankan atau mempertahankan hak di sisi undang-undang;

4.2.5 Pengawal data itu mempunyai alasan yang munasabah untuk mempercayai bahawa dalam segala hal keadaan mengenai hal itu —

(a) pemindahan itu adalah bagi mengelakkan atau mengurangkan tindakan yang memudaratkan terhadap subjek data;

(b) adalah tidak praktikal untuk mendapatkan persetujuan subjek data secara bertulis mengenai pemindahan itu; dan

(c) jika adalah praktikal untuk mendapatkan persetujuan itu, subjek data itu akan memberikan persetujuannya;

4.2.6 Pengawal data itu telah mengambil semua langkah berjaga-jaga yang munasabah dan telah menjalankan segala usaha wajar untuk memastikan bahawa data peribadi itu tidak akan diproses di tempat itu mengikut apa-apa cara yang, sekiranya tempat itu ialah Malaysia, akan menjadi suatu pelanggaran Akta 709; atau

4.2.7 pemindahan itu perlu untuk melindungi kepentingan vital subjek data.

4.3 Sekiranya pengawal data menjalankan atau berhasrat untuk menjalankan pemindahan data peribadi ke luar Malaysia, pengawal data hendaklah melalui notis perlindungan data peribadi atau mana-mana notis bertulis lain memaklumkan subjek data berkenaan pemindahan tersebut.

4.4 Pesuruhjaya boleh menjalankan siasatan terhadap pengawal data untuk menentukan sama ada mana-mana perbuatan, amalan atau permintaan melanggar Seksyen 129 Akta 709.

5. Suatu undang-undang yang sebahagian besarnya serupa dengan Akta 709

5.1 Pengawal data boleh merujuk kepada perenggan 129(2)(a) Akta 709 jika ia membuat keputusan bahawa tempat yang ingin dipindahkan data peribadi tersebut mempunyai undang-undang yang sebahagian besarnya serupa dengan Akta 709.

5.2 Suatu undang-undang ialah sebahagian besarnya serupa dengan Akta 709 jika kandungan undang-undang tersebut seperti perlindungan, hak dan keperluan-keperluan yang berkaitan dengan pemprosesan termasuk pengumpulan,

penzahiran, penyimpanan dan pemindahan data peribadi rentas sempadan adalah serupa dengan yang diperuntukkan di bawah Akta 709.

5.3 Pengawal data boleh melaksanakan Penilaian Impak Pemindahan ("**TIA**") bagi menyemak undang-undang perlindungan data peribadi yang berkaitan di negara/ bidang kuasa penerima setara dengan Akta 709 untuk menepati keperluan yang ditetapkan di bawah perenggan 129(2)(a) Akta 709. TIA tersebut hendaklah dilaksanakan mengikut langkah-langkah berikut:

5.3.1 mengenal pasti negara-negara ke mana data peribadi akan dipindahkan;

5.3.2 menilai undang-undang perlindungan data peribadi di setiap negara yang menerima berdasarkan faktor-faktor yang disenaraikan dalam perenggan 5.4;

5.3.3 tentukan sama ada terdapat undang-undang yang berkuat kuasa yang sebahagian besarnya serupa dengan Akta 709; dan

5.3.4 memastikan bahawa keputusan pemindahan data peribadi mematuhi Akta 709.

5.4 Pengawal data hendaklah sekurang-kurangnya mempertimbangkan faktor-faktor berikut:

5.4.1 sama ada undang-undang tersebut menyediakan hak-hak yang serupa kepada subjek data seperti hak untuk mengakses dan hak untuk membetulkan data peribadi;

5.4.2 sama ada terdapat Prinsip Perlindungan Data Peribadi yang serupa seperti Prinsip Keselamatan;

5.4.3 sama ada terdapat keperluan dan perlindungan yang serupa berkaitan dengan pemprosesan data peribadi termasuk pengumpulan, penzahiran, penyimpanan dan pemindahan rentas sempadan;

5.4.4 sama ada terdapat keperluan serupa atau setara berkaitan Pegawai Perlindungan Data;

5.4.5 sama ada terdapat keperluan serupa berkaitan pemberitahuan pelanggaran data;

5.4.6 sama ada terdapat keperluan serupa yang dikenakan ke atas pemproses data untuk melindungi data peribadi; dan

5.4.7 sama ada wujudnya sebuah badan kawal selia di negara tersebut yang serupa dengan Jabatan Perlindungan Data Peribadi dan mempunyai kuasa-kuasa yang serupa untuk membolehkannya menguatkuasakan undang-undang perlindungan data peribadi yang relevan dengan berkesan.

5.5 TIA tersebut boleh dijalankan dengan merujuk kepada sumber maklumat berikut:

5.5.1 undang-undang, peraturan, garis panduan dan pekeliling yang berkaitan dengan perlindungan data peribadi;

5.5.2 kes perundangan atau keputusan yang diambil oleh badan kehakiman atau pihak berkuasa pentadbiran yang bebas berkaitan isu-isu perlindungan data peribadi;

5.5.3 laporan daripada organisasi antara kerajaan, badan pemantau bebas, persatuan perniagaan dan perdagangan dan badan profesional;

5.5.4 laporan berita mengenai pelanggaran data;

5.5.5 laporan yang disediakan oleh penerima yang berkaitan dengan amalan-amalan dan sejarah perlindungan data peribadi pengawal data/ pemproses data tersebut;

5.5.6 artikel penyelidikan berkaitan undang-undang dan amalan perlindungan data peribadi negara/ bidang kuasa penerima; dan

5.5.7 sumber maklumat lain yang dipercayai dan tidak lapuk yang berkaitan dengan perlindungan data peribadi.

5.6 Dapatan TIA adalah sah untuk tempoh tidak lebih daripada tiga (3) tahun. Selepas tempoh tersebut, pengawal data hendaklah menjalankan TIA susulan mengikut langkah-langkah yang dinyatakan dalam perenggan 5.3.

5.7 Sekiranya terdapat perubahan atau pindaan terhadap undang-undang perlindungan data peribadi yang berkaitan dalam tempoh sah TIA, pengawal data hendaklah menjalankan semakan terhadap perubahan atau pindaan tersebut untuk menentukan sama ada, akibat daripada perubahan atau pindaan tersebut, undang-undang perlindungan data peribadi yang berkaitan masih sebahagian besarnya serupa dengan Akta 709.

6. Suatu tempat dengan tahap perlindungan yang mencukupi

6.1 Pengawal data boleh merujuk kepada perenggan 129(2)(b) Akta 709 jika ia membuat keputusan bahawa tempat di mana data peribadi akan dipindahkan mampu memastikan bahawa semua data peribadi yang dipindahkan kepadanya akan diberikan tahap perlindungan yang mencukupi yang sekurang-kurangnya setara dengan tahap perlindungan yang diberikan oleh Akta 709.

6.2 Pengawal data boleh melaksanakan TIA bagi menentukan tahap perlindungan data peribadi yang ditawarkan di negara/ bidang kuasa penerima setara dengan Akta 709 untuk menepati keperluan yang ditetapkan di bawah perenggan 129(2)(b) Akta 709. TIA hendaklah dilaksanakan mengikut langkah-langkah berikut:

6.2.1 mengenal pasti negara-negara di mana data peribadi akan dipindahkan;

6.2.2 menilai mekanisme untuk melindungi data peribadi di setiap negara/ bidang kuasa penerima berdasarkan faktor-faktor yang disenaraikan dalam perenggan 6.3;

6.2.3 berdasarkan dapatan TIA, tentukan:

(a) sama ada terdapat langkah-langkah perlindungan untuk memastikan data peribadi diberikan tahap perlindungan yang mencukupi setara dengan Akta 709; dan

(b) sama ada terdapat langkah-langkah tambahan yang mesti diambil oleh penerima untuk memastikan data peribadi dilindungi dengan mencukupi; dan

6.2.4 memastikan bahawa keputusan pemindahan data peribadi mematuhi Akta 709.

6.3 Pengawal data hendaklah mempertimbangkan faktor-faktor berikut:

6.3.1 sama ada penerima menggunapakai langkah dan dasar keselamatan yang selaras dengan Prinsip Keselamatan dan Standard Perlindungan Data Peribadi;

6.3.2 sama ada penerima menggunapakai sebarang pensijilan berkaitan keselamatan yang telah menilai sistem-sistem yang digunapakai dan didapati selamat;

6.3.3 sama ada penerima terikat dengan obligasi yang boleh dikuatkuasakan di sisi undang-undang (sama ada melalui kontrak, perjanjian atau undang-undang) dan sama ada obligasi tersebut boleh dikuatkuasakan oleh pengawal data atau subjek data yang data peribadinya akan dipindahkan kepada penerima tersebut;

6.3.4 sama ada undang-undang perlindungan data peribadi yang mentadbir penerima boleh dikuatkuasakan dengan mudah;

6.3.5 sejarah pematuhan undang-undang perlindungan data peribadi oleh penerima dan sama ada mereka pernah mengalami sebarang insiden pelanggaran data;

6.3.6 sama ada pengawal data penerima mengenakan atau dikehendaki di bawah undang-undang bagi mengenakan keperluan terhadap pemproses data untuk melindungi data peribadi; dan

6.3.7 sama ada terdapat badan kawal selia yang serupa dengan Jabatan Perlindungan Data Peribadi yang melaksanakan fungsi dan menjalankan kuasa di bawah undang-undang berkaitan perlindungan data peribadi.

6.4 TIA tersebut boleh dijalankan dengan merujuk kepada sumber maklumat yang disenaraikan di bawah perenggan 5.5.

6.5 Dapatan TIA adalah sah untuk tempoh tidak lebih daripada tiga (3) tahun. Selepas tempoh tersebut, pengawal data hendaklah menjalankan TIA susulan mengikut langkah-langkah yang dinyatakan dalam perenggan 6.2.

6.6 Sekiranya terdapat perubahan atau pindaan yang signifikan kepada sistem atau dasar yang berkaitan dengan keselamatan dan perlindungan data peribadi dalam tempoh sah TIA, pengawal data hendaklah menyemak perubahan atau pindaan tersebut untuk menentukan sama ada, hasil daripada perubahan atau pindaan tersebut, data peribadi masih diberikan perlindungan mencukupi yang bersamaan dengan Akta 709.

7. Persetujuan subjek data terhadap pemindahan data peribadi

7.1 Pengawal data boleh merujuk kepada perenggan 129(3)(a) Akta 709 bagi pemindahan data peribadi rentas sempadan jika subjek data telah memberikan persetujuan terhadap pemindahan tersebut.

7.2 Pengawal data hendaklah terlebih dahulu memberikan notis perlindungan data peribadi kepada subjek data yang mengandungi maklumat berikut mengenai pemindahan data peribadi rentas sempadan:

(a) golongan pihak ketiga yang kepadanya data dipindahkan; dan

(b) tujuan pemindahan tersebut.

7.3 Selepas subjek data diberikan notis perlindungan data peribadi, pengawal data hendaklah mendapatkan persetujuan subjek data terhadap pemindahan data peribadi tersebut. Persetujuan tersebut hendaklah direkodkan dan disenggara dengan sewajarnya mengikut keperluan Peraturan-Peraturan Perlindungan Data Peribadi.

8. Pemindahan yang perlu bagi pelaksanaan kontrak antara subjek data dan pengawal data

8.1 Pengawal data yang mempunyai kontrak dengan subjek data boleh merujuk kepada perenggan 129(3)(b) Akta 709 bagi pemindahan data peribadi rentas sempadan jika:

8.1.1 berdasarkan faktor-faktor yang disenaraikan dalam perenggan 8.3 dan 8.4, pemindahan adalah perlu untuk pengawal data melaksanakan obligasi-obligasi dalam kontrak; dan

8.1.2 obligasi-obligasi tersebut hendaklah untuk tujuan utama kontrak.

8.2 Perlu ada hubungan langsung dan objektif antara pelaksanaan kontrak dan pemindahan data peribadi rentas sempadan.

Keperluan pemindahan data peribadi rentas sempadan

8.3 Perkataan ‘perlu’ yang terkandung dalam perenggan 129(3)(b), (c) dan (g) Akta 709 tidak bermakna pemindahan data peribadi rentas sempadan itu amat mustahak. Walau bagaimanapun, pemindahan data peribadi rentas sempadan hendaklah memenuhi faktor-faktor berikut:

8.3.1 pemindahan data peribadi rentas sempadan bukan sekadar amalan atau dilakukan secara tetap. Sebab-sebab bagi pemindahan tersebut hendaklah untuk memenuhi tujuan tertentu yang ditetapkan dan bukannya untuk tujuan umum atau amalan syarikat;

Contoh:

Sebuah agensi pelancongan yang berniat untuk memindahkan data peribadi pelanggan mereka ke luar negara mungkin tidak boleh bergantung pada hujah bahawa ia adalah amalan industri untuk memindahkan data peribadi ke luar Malaysia atau bahawa tujuan pemindahan tersebut adalah untuk rekod agensi pelancongan atau penyelenggaraan pangkalan data pelanggan mereka.

Sebaliknya, agensi pelancongan tersebut boleh dikatakan memindahkan data peribadi ke luar Malaysia untuk tujuan yang ditetapkan jika pemindahan tersebut adalah untuk tujuan tempahan penginapan atau tiket acara untuk pelanggan mereka.

8.3.2 pemindahan data peribadi rentas sempadan dibuat untuk mencapai tujuan tertentu sahaja dan bukan untuk tujuan umum; dan

Penjelasan:

Satu pemindahan dianggap dilakukan untuk mencapai tujuan tertentu jika pengawal data dapat membuktikan bahawa pemindahan tersebut dilakukan untuk memenuhi tujuan tertentu. Tujuan tertentu ini tidak seharusnya semata-mata untuk manfaat pengawal data dan perlu spesifik untuk subjek data atau kumpulan kecil subjek data berbanding dengan semua subjek data pengawal data tersebut.

8.3.3 pengawal data tidak dapat mencapai tujuan yang dinyatakan melalui mana-mana alternatif yang boleh dilaksanakan dengan munasabah.

Penjelasan:

Pengawal data akan dianggap mempunyai "cara alternatif yang boleh dilaksanakan" jika cara alternatif tersebut:

(a) boleh dilaksanakan dengan kos yang lebih rendah atau serupa; dan
(b) mampu mencapai keputusan atau hasil yang serupa.

Sebagai contoh, pengawal data yang ingin menyimpan data peribadi di pusat data di luar Malaysia akan dianggap mempunyai cara alternatif yang boleh dilaksanakan jika terdapat pusat data tempatan yang menawarkan perkhidmatan penyimpanan data pada kos yang lebih rendah atau serupa.

8.4 Apabila membuat penilaian sama ada pemindahan data peribadi rentas sempadan memenuhi faktor-faktor di atas, pengawal data harus mengambil kira perkara berikut:

8.4.1 sebab mengapa pemindahan diperlukan;

8.4.2 tujuan pemindahan tersebut; dan

8.4.3 sama ada terdapat sebarang alternatif yang boleh dilaksanakan.

Bagi tujuan teras kontrak

8.5 Pemindahan data peribadi mesti berkait secara langsung dengan dan untuk tujuan melaksanakan obligasi-obligasi pengawal data seperti yang dinyatakan di bawah kontrak.

9. Pemindahan yang diperlukan untuk penyempurnaan atau pelaksanaan kontrak antara pengawal data dan pihak ketiga

9.1 Pengawal data boleh merujuk kepada perenggan 129(3)(c) Akta 709 bagi pemindahan data peribadi rentas sempadan jika:

9.1.1 pemindahan itu perlu bagi penyempurnaan atau pelaksanaan kontrak antara pengawal data dan pihak ketiga;

9.1.2 kontrak tersebut:

(a) dimasuki di atas permintaan subjek data; atau

(b) adalah demi kepentingan subjek data;

9.1.3 berdasarkan faktor-faktor yang disenaraikan di bawah perenggan 8.3 dan 8.4, pemindahan adalah perlu untuk penyempurnaan atau pelaksanaan kontrak.

9.2 Permintaan oleh subjek data yang dirujuk dalam perenggan 9.1.2(a) perlu:

9.2.1 disediakan dalam bentuk bertulis; atau

9.2.2 di mana permintaan itu dibuat melalui cara-cara selain daripada secara bertulis, permintaan tersebut disenggara dan disimpan dalam bentuk yang sepatutnya yang boleh ditunjukkan sebagai bukti bahawa subjek data membuat permintaan tersebut.

9.3 Pengawal data yang berhasrat untuk merujuk kepada perenggan 9.1.2(b) (kepentingan subjek data) hanya boleh berbuat demikian jika kepentingan subjek data ditunjukkan secara:

9.3.1 jelas dan penting: hendaklah ada faedah yang jelas yang boleh dikenal pasti dan dinyatakan dengan jelas oleh pengawal data;

9.3.2 langsung: hasil daripada penyempurnaan atau pelaksanaan kontrak memberi faedah secara langsung kepada subjek data; dan

9.3.3 disasarkan kepada subjek data: matlamat atau tujuan utama kontrak hendaklah memberikan faedah secara langsung kepada subjek data.

Contoh:

Subjek data membeli pakej pelancongan untuk keluarganya. Agensi pelancongan kemudian memasuki kontrak dengan pengendali (seperti pengendali hotel dan penerbangan) dan seterusnya memindahkan data peribadi mereka ke luar Malaysia kepada pengendali tersebut bagi tujuan membuat tempahan perjalanan. Ini dianggap sebagai faedah yang jelas, langsung dan bersasar kerana kontrak:

(a) mempunyai faedah yang jelas: Subjek data dan keluarganya akan dapat bercuti dengan hotel dan penerbangan mereka yang ditempah lebih awal;

(b) adalah langsung: Pelaksanaan kontrak antara agensi pelancongan dan pengendali memberikan faedah langsung kepada subjek data dan keluarganya; dan

(c) disasarkan kepada subjek data: matlamat utama kontrak antara agensi pelancongan dan pengendali adalah untuk memastikan subjek data dan keluarganya dapat bercuti. Kontrak juga disasarkan kepada subjek data dan keluarganya.

9.4 Sebagai tambahan, pengawal data hendaklah mempertimbangkan faktor-faktor yang disenaraikan di bawah perenggan 8.3 dan 8.4 berhubung dengan penyempurnaan atau pelaksanaan kontrak antara pengawal data dan pihak ketiga untuk memastikan bahawa pemindahan itu diperlukan.

10. Pemindahan untuk tujuan prosiding undang-undang

10.1 Pengawal data boleh merujuk kepada perenggan 129(3)(d) Akta 709 untuk pemindahan data peribadi rentas sempadan jika pemindahan itu adalah untuk tujuan:

10.1.1 prosiding undang-undang;

10.1.2 mendapatkan nasihat undang-undang; atau

10.1.3 mewujudkan, menjalankan atau mempertahankan hak di sisi undang-undang.

10.2 Prosiding undang-undang adalah termasuk perkara berikut:

10.2.1 suatu tuntutan yang akan dibawa dan dipertahankan di dalam sesuatu mahkamah (termasuk undang-undang sivil dan jenayah);

10.2.2 suatu tuntutan yang akan dibawa dan dipertahankan di tribunal (contohnya, sebuah tribunal tuntutan pengguna);

10.2.3 prosedur pentadbiran atau pengawalseliaan (contohnya, untuk mempertahankan suatu penyiasatan (atau penyiasatan yang berpotensi untuk timbul) dalam undang-undang persaingan atau perkhidmatan kewangan, atau untuk mendapatkan kelulusan untuk suatu penggabungan); atau

10.2.4 suatu prosedur luar mahkamah (contohnya, mesyuarat tanpa prejudis, pengantaraan atau timbang tara).

10.3 Pengawal data tidak boleh merujuk kepada syarat di bawah perenggan 129(3)(d) jika hanya ada kemungkinan bahawa prosiding undang-undang atau prosiding-prosiding rasmi lain boleh dibawa pada masa hadapan. Walau bagaimanapun, pengawal data boleh merujuk kepada syarat ini jika pengawal data:

10.3.1 terlibat dalam surat-menyurat pra-tindakan;

10.3.2 mengambil nasihat tentang risiko undang-undang dalam membawa atau mempertahankan suatu tuntutan; atau

10.3.3 telah menerima permintaan untuk maklumat daripada badan kawal selia luar negara kerana badan kawal selia tersebut berpotensi mengambil tindakan rasmi.

11. Alasan munasabah pengawal data

11.1 Pengawal data boleh merujuk kepada perenggan 129(3)(e) Akta 709 bagi pemindahan data peribadi rentas sempadan jika ia mempunyai alasan yang munasabah untuk mempercayai bahawa:

11.1.1 pemindahan itu adalah untuk mengelakkan atau mengurangkan tindakan yang memudaratkan terhadap subjek data;

11.1.2 adalah tidak praktikal untuk mendapatkan persetujuan subjek data secara bertulis mengenai pemindahan itu; dan

11.1.3 jika adalah praktikal untuk mendapatkan persetujuan itu, subjek data itu akan memberikan persetujuannya.

11.2 Perenggan 129(3)(e) Akta 709 hanya terpakai jika subjek data tidak boleh memberikan persetujuan mereka seperti berikut:

11.2.1 subjek data tidak sedar diri;

11.2.2 subjek data tidak dapat dihubungi dan memandangkan keadaan, langkah yang munasabah dan berkadar telah diambil dalam percubaan untuk menghubungi mereka; atau

11.2.3 subjek data tidak dapat memberikan persetujuan kerana masa yang tidak mencukupi untuk penyediaan semua maklumat yang diperlukan bagi persetujuan tersebut.

12. Keperluan untuk mengambil semua langkah berjaga-jaga yang munasabah dan menjalankan semua usaha wajar untuk pemindahan data peribadi rentas sempadan

12.1 Pengawal data boleh merujuk kepada perenggan 129(3)(f) Akta 709 untuk sebarang pemindahan data peribadi rentas sempadan jika pengawal data telah mengambil semua langkah berjaga-jaga yang munasabah dan menjalankan semua usaha wajar untuk memastikan bahawa data peribadi itu tidak akan diproses di tempat itu dalam apa-apa cara yang, sekiranya tempat itu adalah

Malaysia, akan menjadi suatu pelanggaran Akta 709. Dalam hal ini, semua langkah berjaga-jaga yang munasabah serta usaha wajar boleh ditentukan melalui mekanisme berikut:

12.1.1 Peraturan Korporat Yang Mengikat ("**BCR**");

12.1.2 Klausa-Klausa Kontrak ("**CC**"); atau

12.1.3 Pensijilan di bawah sesuatu skim pensijilan yang diluluskan ("**Pensijilan**").

Peraturan Korporat Yang Mengikat

12.2 BCR ialah dasar perlindungan data peribadi yang dilaksanakan oleh kumpulan korporat multinasional, kumpulan usaha (*undertakings*) atau kumpulan perniagaan perusahaan (*enterprise*) yang terlibat dalam aktiviti ekonomi secara bersama seperti francais, usaha sama atau perkongsian profesional.

12.3 Pengawal data boleh merujuk kepada BCR yang terpakai kepada pengawal data dan penerima untuk sebarang pemindahan data peribadi rentas sempadan yang bersifat intra-kumpulan.

Penjelasan:

Pengawal data boleh menjalankan pemindahan data peribadi rentas sempadan kepada francaisor atau anak syarikatnya di mana terdapat BCR yang dilaksanakan oleh kedua-dua pengawal data dan penerima.

12.4 Keperluan untuk BCR ialah:

12.4.1 BCR mengandungi butiran-butiran berikut:

(a) pihak-pihak yang dikawal di bawah BCR;

(b) negara/ bidang kuasa yang ditetapkan di mana data peribadi boleh dipindahkan;

(c) sifat BCR yang mengikat secara sah kepada semua pihak-pihak BCR dan kepada mana-mana subjek data di bawah pihak-pihak BCR berhubung dengan pemindahan data yang dibuat di bawah BCR;

(d) keperluan bagi pihak-pihak untuk memastikan satu standard perlindungan yang bersamaan dengan Akta 709;

(e) keperluan untuk mematuhi prinsip-prinsip perlindungan data peribadi;

(f) tempoh penyimpanan data peribadi;

(g) pelaporan tentang sebarang pelanggaran data peribadi;

(h) mekanisme untuk memastikan pematuhan;

(i) pembahagian liabiliti untuk sebarang pelanggaran data peribadi;

(j) keperluan atau sekatan yang berkaitan dengan pemindahan data peribadi kepada mana-mana pembekal perkhidmatan pihak ketiga;

(k) hak-hak subjek data dan kaedah-kaedah untuk melaksanakan hak mereka;

(l) pelaksanaan audit untuk memastikan pematuhan oleh setiap pihak;

(m) tarikh kuat kuasa dan tarikh semakan terakhir BCR;

(n) tanggungjawab Pegawai Perlindungan Data atau mana-mana individu yang bertanggungjawab untuk memantau pematuhan terhadap BCR; dan

(o) prosedur aduan.

12.4.2 BCR mengikat secara sah ke atas semua pihak dalam kontrak dan dapat dikuatkuasakan; dan

12.4.3 BCR disemak dari semasa ke semasa untuk memastikan bahawa ia dikemas kini.

12.5 Sebarang semakan terhadap BCR hendaklah mengambil kira perkembangan terkini dalam undang-undang perlindungan data yang relevan. Pengawal data juga digalakkan untuk melantik juruaudit bebas untuk menyemak BCR bagi memastikan pematuhan terhadap Akta 709.

Klausa-klausa kontrak

12.6 CC ialah satu set klausa yang dimasukkan ke dalam suatu kontrak yang akan mengikat secara sah kepada kedua-dua pengawal data dan penerima untuk memastikan suatu tahap perlindungan yang mencukupi berhubung dengan pemprosesan data peribadi.

12.7 Pengawal data yang berhasrat untuk mematuhi CC hendaklah memastikan bahawa CC tersebut sekurang-kurangnya, merangkumi perkara berikut:

12.7.1 langkah-langkah keselamatan yang akan dilaksanakan untuk menyediakan suatu tahap perlindungan yang mencukupi berhubung dengan pemprosesan data peribadi yang sekurang-kurangnya setara dengan tahap perlindungan yang diberikan oleh Akta 709; dan

12.7.2 klausa-klausa yang menyatakan dan menjamin bahawa pemprosesan data peribadi hendaklah dijalankan dengan mematuhi Akta 709.

12.8 Pengawal data yang bergantung kepada penggunaan CC hendaklah pada setiap masa mengambil segala langkah berjaga-jaga yang munasabah bagi memastikan bahawa penerima mematuhi terma-terma yang diperuntukkan dalam CC. Sekiranya pengawal data mendapati terdapat suatu perlanggaran terhadap terma-terma CC, pengawal data hendaklah menghentikan pemindahan data peribadi kepada pihak-pihak lain dalam kontrak sehingga pihak berkenaan membetulkan pelanggaran tersebut.

Penggunaan Model Antarabangsa

12.9 Pengawal data yang berhasrat untuk menggunakan model antarabangsa boleh menerima pakai senarai klausa kontrak berikut, termasuk tetapi tidak terhad kepada:

12.9.1 *Association of Southeast Asian Nations (ASEAN) Model Contractual Clauses for Cross Border Data Flows*;

12.9.2 *General Data Protection Regulation (EU GDPR) Standard Contractual Clauses for the Transfer of Personal Data to Third Countries*; dan

12.9.3 CC lain seperti yang ditentukan oleh Pesuruhjaya dari semasa ke semasa.

12.10 Sebelum sebarang penggunaan model antarabangsa di atas, pengawal data disarankan untuk membuat semakan ke atas CC bagi menentukan sama ada sebarang klausa tambahan diperlukan untuk memastikan tahap perlindungan yang mencukupi yang sekurang-kurangnya setara dengan tahap perlindungan yang diberikan oleh Akta 709.

Pensijilan

12.11 Pengawal data/ pemproses data boleh mendapatkan pensijilan berkaitan perlindungan data peribadi sebagai kaedah perakuan bahawa pengawal data/ pemproses data tersebut mempunyai dasar dan proses yang mencukupi untuk mematuhi standard/ undang-undang perlindungan data atau menyediakan tahap perlindungan yang mencukupi untuk melindungi data peribadi.

Contoh:

- *Europrivacy* ialah skim pensijilan yang diuruskan oleh *European Centre For Certification and Privacy* dan direka untuk menilai, mendokumentasikan, memperakui dan menilai pematuhan EU GDPR.

- *Legal Services Operational Privacy Certification Scheme* direka untuk membantu penyedia perkhidmatan undang-undang menunjukkan pematuhan undang-undang perlindungan data di United Kingdom apabila memproses data peribadi pelanggan mereka.

- *Asia Pacific Economic Cooperation Cross Border Privacy Rules System* ("APEC CBPR") dan Pensijilan *Privacy Recognition for Processors* ("APEC PRP") adalah dikeluarkan oleh *Infocomm Media Development Authority* (Singapura) dan *TrustArc* untuk memperakui bahawa dasar dan proses perlindungan pengawal data/ pemproses data mematuhi Prinsip APEC CBPR dan APEC PRP.

12.12 Pengawal data boleh merujuk kepada syarat di bawah perenggan 129(3)(f) Akta 709 untuk memindahkan data peribadi ke luar Malaysia jika:

12.12.1 penerima memiliki Sijil Diiktiraf yang sah;

12.12.2 pengawal data menjalankan usaha-usaha yang munasabah untuk mengesahkan kesahihan Sijil Diiktiraf;

Contoh:

Usaha-usaha yang munasabah untuk mengesahkan kesahihan sijil termasuk:

(a) mendapatkan salinan Sijil Diiktiraf yang disahkan benar; dan

(b) jika boleh, mengesahkan kesahihan Sijil Diiktiraf melalui pangkalan data dalam talian. Sebagai contoh, *Europrivacy* mempunyai Pendaftaran Sijil yang membolehkan orang ramai mencari dan mengesahkan kesahihan Sijil Diiktiraf.

12.12.3 pengawal data memasuki kontrak dengan penerima yang:

i. mengenakan suatu obligasi ke atas penerima untuk memastikan bahawa ianya mempunyai tahap perlindungan yang mencukupi untuk melindungi data peribadi yang dipindahkan kepada mereka; dan

ii. menjamin bahawa Sijil Diiktiraf adalah sah.

12.13 Pengawal data hendaklah pada setiap masa mengambil semua langkah berjaga-jaga yang munasabah untuk memastikan bahawa penerima mematuhi obligasi-obligasinya untuk melindungi data peribadi. Sekiranya pengawal data menemui terdapatnya pelanggaran obligasi-obligasi tersebut, pengawal data tersebut hendaklah menghentikan pemindahan data peribadi kepada penerima sehingga pelanggaran itu telah diperbetulkan.

13. Pemindahan yang diperlukan untuk melindungi kepentingan vital subjek data

Kepentingan Vital Subjek Data

13.1 Pengawal data boleh merujuk kepada perenggan 129(3)(g) Akta 709 untuk sebarang pemindahan data peribadi rentas sempadan jika:

13.1.1 keperluan pemindahan memenuhi faktor-faktor yang dinyatakan di bawah perenggan 8.3 dan 8.4; dan

13.1.2 tujuan pemindahan data peribadi rentas sempadan adalah untuk melindungi kepentingan vital subjek data.

13.2 Walau apa pun perenggan 13, risiko kepada kepentingan vital subjek data hendaklah menjangkaui sebarang kepentingan perlindungan data peribadi.

Contoh:

Pengawal data boleh bergantung kepada perenggan 129(3)(g) Akta 709 bagi pemindahan data peribadi rentas sempadan jika subjek data warganegara Malaysia berada dalam keadaan koma di Singapura dan data peribadi tentang sejarah perubatannya perlu dipindahkan ke Singapura untuk rawatan perubatan yang perlu.

Jika subjek data tersebut sedar diri dan mampu memberikan persetujuan, dan pengawal data mempunyai masa yang mencukupi untuk mendapatkan persetujuan, pemindahan data peribadi rentas sempadan adalah tidak memenuhi perenggan 129(3)(g) Akta 709.

BAHAGIAN C: PENGENDALIAN PEMINDAHAN DATA PERIBADI RENTAS SEMPADAN

14. Tanggungjawab pengawal data apabila memindahkan data peribadi

14.1 Pengawal data bertanggungjawab ke atas keselamatan data peribadi apabila memindahkan ke luar Malaysia dan hendaklah mengambil langkah-langkah praktikal untuk melindungi data peribadi daripada sebarang kehilangan, penyalahgunaan, pengubahsuaian, akses ataupun penzahiran yang tidak dibenarkan atau tidak disengajakan, pengubahan atau pemusnahan.

14.2 Pengawal data hendaklah memastikan bahawa kaedah pemindahan data peribadi ke luar Malaysia adalah selamat dan selaras dengan Prinsip Keselamatan di bawah Akta 709, perundangan subsidiari, standard dan garis panduan lain yang berkaitan dengan perlindungan data peribadi.

15. Berurusan dengan pihak ketiga/ pemproses data

15.1 Pengawal data hendaklah memastikan bahawa sebarang kontrak dengan pihak ketiga/ pemproses data mengandungi klausa-klausa yang mentadbir pemprosesan data peribadi, termasuk keselamatan data peribadi.

15.2 Pengawal data hendaklah memastikan bahawa pemproses data mematuhi Seksyen 9 Akta 709, perundangan subsidiari, standard dan garis panduan lain yang berkaitan dengan perlindungan data peribadi.

16. Penyimpanan rekod

16.1 Pengawal data yang menjalankan pemindahan data peribadi rentas sempadan hendaklah menyimpan dan mengekalkan rekod penerima data peribadi yang dipindahkan. Rekod sedemikian hendaklah mengandungi butiran-butiran berikut:

16.1.1 butiran penerima data peribadi sekurang-kurangnya seperti yang berikut:

(a) nama penerima;

(b) nombor pendaftaran syarikat (jika ada); dan

(c) butiran perhubungan Pegawai Perlindungan Data atau orang lain di pihak penerima;

16.1.2 negara di mana data peribadi dipindahkan;

16.1.3 jenis data peribadi yang dipindahkan;

16.1.4 tujuan pemindahan; dan

16.1.5 maklumat lain yang difikirkan perlu oleh pengawal data.

16.2 Sebagai tambahan, pengawal data yang menjalankan pemindahan data peribadi rentas sempadan hendaklah menyimpan dan menyenggara rekod yang boleh membuktikan dengan secukupnya bahawa setiap pemindahan data peribadi rentas sempadan mematuhi Seksyen 129 Akta 709. Contoh-contoh rekod sedemikian termasuk:

Syarat-syarat	Rekod
Subseksyen 129(2) Akta 709	- Rekod TIA; dan - Dapatan TIA tersebut.
Perenggan 129(3)(a) Akta 709	- Notis perlindungan data peribadi; dan - Rekod persetujuan subjek data.
Diperlukan bagi pelaksanaan kontrak	- Salinan kontrak; dan - Bukti bahawa pemprosesan itu perlu untuk pelaksanaan kontrak.
Langkah berjaga-jaga yang munasabah	- Salinan BCR; - Salinan Sijil Diiktiraf; atau - Salinan kontrak yang ditandatangani antara Pengawal Data dan penerima.

16.3 Pengawal data hendaklah menyimpan dan menyenggara rekod yang disediakan di bawah perenggan 16.1 tertakluk kepada Prinsip Penyimpanan di bawah Akta 709, perundangan subsidiari, standard dan garis panduan lain yang berkaitan dengan perlindungan data peribadi atau undang-undang lain yang berkuatkuasa.

MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION

GUIDELINES

CROSS BORDER PERSONAL DATA TRANSFER (CBPDT)

Version 1.0

Date of Issuance: 29 April 2025

PERSONAL DATA PROTECTION COMMISSIONER MALAYSIA

Address:

PERSONAL DATA PROTECTION COMMISSIONER OF MALAYSIA

Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana

Precinct 4, Federal Government Administration Centre

62100 Putrajaya, Malaysia

TABLE OF CONTENTS

PART A: INTRODUCTION

1. Background

1.1 Section 129 of the Personal Data Protection Act 2010 [Act 709] (**"Act 709"**) regulates the transfer of personal data out of Malaysia. In order to carry out cross border personal data transfer, data controller is required to comply with the provisions under Section 129 of the Act 709.

1.2 This Guideline sets out as a guidance to clarify the requirements for compliance with each condition specified under Section 129 of the Act 709 and to assist data controller in deciding which condition may be referred to for any cross border personal data transfer.

1.3 Please note that the examples provided in this Guideline are not intended to be exhaustive and are only included for context and for purposes of illustration.

1.4 This guideline supplements and is to be read together with Act 709 and any other relevant legislative instrument(s) issued under the Act 709, as may be amended from time to time. It should not be considered to override any other data protection-related laws and regulations in effect at any given time.

2. Legal Provisions

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

3. Interpretation

3.1 Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings assigned to them under the Act 709 and any other relevant legislative instruments under the Act 709.

3.2 In these Guidelines, unless the context otherwise requires:

"Personal data protection notice"	means a notice in writing that the data controller is required to provide to the data subject in compliance with Section 7 of Act 709;
"Receiver"	means data controller and/ or data processor who receives personal data of subject data outside of Malaysia;
"Transfer Impact Assessment"	means is a risk assessment conducted to evaluate the legal and regulatory framework where personal data is being transferred to ensure that receiving country/ jurisdiction provides a law substantially similar to Act 709 or adequate level of protection in relation to the processing of personal data;
"Recognised Certificate"	means certificate issued by an accredited body or authority that verifies that a data controller or data processor is in compliance with data protection standards or laws, both locally or internationally.

PART B: CONDITIONS FOR THE TRANSFER OF PERSONAL DATA TO PLACES OUTSIDE MALAYSIA

4. Conditions for cross border personal data transfer

4.1 Subsection 129(2) of the Act 709 provides that a data controller may transfer any personal data of a data subject to any place outside Malaysia if:

(a) there is in that place in force any law which is substantially similar to the Act 709; or

(b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the Act 709.

4.2 Notwithstanding subsection 129(2) of the Act 709, data controller may transfer any personal data to a place outside Malaysia if:

4.2.1 data subject has given consent to the transfer;

4.2.2 the transfer is necessary for the performance of a contract between data subject and data controller;

4.2.3 the transfer is necessary for the conclusion or performance of a contract between data controller and third party which —

(a) is entered into at the request of data subject; or

(b) is in the interests of data subject;

4.2.4 the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;

4.2.5 the data controller has reasonable grounds for believing that in all circumstances of the case —

(a) the transfer is for the avoidance or mitigation of adverse action against the data subject;

(b) it is not practicable to obtain the consent in writing of the data subject to that transfer; and

(c) if it was practicable to obtain such consent, the data subject would have given his consent;

4.2.6 the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the Act 709; or

4.2.7 the transfer is necessary in order to protect the vital interests of the data subject.

4.3 In the event that data controller carries out or intends to carry out the transfer of personal data out of Malaysia, the data controller shall through its personal data protection notice or such other written notice inform data subject about the transfer.

4.4 The Commissioner may conduct an investigation on data controller to ascertain whether any act, practice or request contravenes Section 129 of Act 709.

5. A law substantially similar to the Act 709

5.1 Data controller may refer to paragraph 129(2)(a) of the Act 709 if it makes a finding that the place it intends to transfer personal data to has in place a law substantially similar to the Act 709.

5.2 A law is substantially similar to the Act 709 if the content of the law such as protection, rights and requirements related to processing including collection, disclosure, retention and cross border personal data transfer are similar to that provided under the Act 709.

5.3 Data controller may conduct Transfer Impact Assessment ("**TIA**") to review the relevant personal data protection law of the receiving country/ jurisdiction is equivalent to the Act 709 in order to fulfil the requirement under paragraph 129(2)(a) of the Act 709. The TIA shall be carried out in accordance with the following steps:

5.3.1 identify the countries to which the personal data is to be transferred to;

5.3.2 assess the personal data protection laws available in each of the receiving countries based on the factors listed in Paragraph 5.4;

5.3.3 determine whether there is in force a law substantially similar to the Act 709; and

5.3.4 ensure that the decision to transfer personal data comply with the Act 709.

5.4 Data controller shall at a minimum consider the following factors:

5.4.1 whether the law provides data subjects with similar rights such as the right of access and the right to correct personal data;

5.4.2 whether there are similar Personal Data Protection Principles in place such as the Security Principle;

5.4.3 whether there are similar requirement and protection with regards to the processing of personal data including collection, disclosure, retention and cross border data transfer;

5.4.4 whether there is similar or equivalent requirement regarding Data Protection Officer;

5.4.5 whether there is similar data breach notification requirement;

5.4.6 whether there is similar requirement imposed on data processor to protect personal data; and

5.4.7 whether there exists a regulatory authority in that country that is similar to the Department of Personal Data Protection and has similar powers to enable it to effectively enforce the relevant personal data protection law.

5.5 The TIA may be carried out by referring to the following source of information:

5.5.1 the laws, regulations, guidelines and circulars that relate to personal data protection;

5.5.2 case law or decision taken by independent judicial or administrative authorities regarding personal data protection matters;

5.5.3 reports from intergovernmental organisations, independent oversight bodies, business and trade associations and professional bodies;

5.5.4 news reports of data breaches;

5.5.5 reports provided by the receiver relating to the personal data protection practices and history of the said data controller/ data processor;

5.5.6 research articles relating to personal data protection laws and practices of receiving country/ jurisdiction; and

5.5.7 such other sources of information that are credible and not outdated relating to personal data protection.

5.6 The findings of the TIA shall be valid for no longer than three (3) years. Beyond that period, data controller shall conduct follow-up TIA following the steps outlined in paragraph 5.3.

5.7 In the event that there occurs a change or amendment to the relevant personal data protection laws during the validity period of the TIA, data controller shall conduct a review of the changes or amendments made to determine whether, as a result of the change or amendment, the relevant personal data protection law is still substantially similar to the Act 709.

6. A place with an adequate level of protection

6.1 Data controller may refer to paragraph 129 (2)(b) of the Act 709 if it makes a finding that the place it transfers personal data to is able to ensure that all the personal data transferred will be provided with an adequate level of protection that is at least equivalent to the level of protection provided by the Act 709.

6.2 Data controller may conduct TIA to determine the level of protection of personal data offered by the receiving country/ jurisdiction is equivalent to the Act 709 in order to fulfil the requirement under paragraph 129(2)(b) of the Act 709. The TIA shall be carried out in accordance with the following steps:

6.2.1 identify the countries which personal data is to be transferred to;

6.2.2 assess the mechanism to protect personal data of the receiving country/ jurisdiction based on the factors listed in paragraph 6.3;

6.2.3 based on the findings of the TIA determine:

(a) whether there are protection measures in place to ensure that the personal data is provided with an adequate level of protection equivalent to the Act 709; and

(b) whether there are further measures that must be taken by the receiver to ensure that personal data is adequately protected; and

6.2.4 ensure that the decision to transfer personal data comply with the Act 709.

6.3 Data controller shall consider the following factors:

6.3.1 whether the receiver has security measures and policies that are in line with the Security Principle and the Personal Data Protection Standard;

6.3.2 whether the receiver has in place any security related certifications which have assessed the systems in place and deemed to be secure;

6.3.3 whether the receiver is bound by legally enforceable obligations (either through contract, agreement or by law) and whether such obligations can be enforced by the data controller or data subject whose personal data is to be transferred to such receiver;

6.3.4 whether the relevant personal data protection law governing the receiver be easily enforced;

6.3.5 the receiver's past history of compliance with the relevant personal data protection law and whether it has experienced any data breach incidents;

6.3.6 whether the receiver (data controller) imposes or is legally required to impose requirements on data processor to protect personal data; and

6.3.7 whether there is a regulatory authority similar to the Department of Personal Data Protection that performs the functions and exercises powers under the law regarding personal data protection.

6.4 The TIA may be carried out by referring to the sources of information listed under paragraph 5.5.

6.5 The findings of the TIA shall be valid for no longer than three (3) years. Beyond that period, data controller shall conduct follow-up TIA following the steps outlined in paragraph 6.2.

6.6 In the event that there occurs a significant change or amendment to the systems or policies that relate to the security and protection of personal data during the validity period of the TIA, the data controller shall review the changes or amendments made to determine whether, as a result of the change or amendment, personal data is still provided with adequate protection equivalent to the Act 709.

7. Data subject's consent to the personal data transfer

7.1 Data controller may refer to paragraph 129(3)(a) of the Act 709 for cross border personal data transfer if the data subject has given consent to the transfer.

7.2 Data controller must first provide the data subject with personal data protection notice containing the following details regarding the cross border personal data transfer:

(a) the class of third parties to whom the data is transferred to; and

(b) the purpose of the transfer.

7.3 After the data subject has been provided with the personal data protection notice, data controller must obtain consent of data subject for the personal data transfer. The consent must be recorded and maintained in accordance with the requirements of the Personal Data Protection Regulations.

8. Transfer necessary for the performance of a contract between data subject and data controller

8.1 Data controller who has contract with data subject may refer to paragraph 129(3)(b) of the Act 709 for cross border personal data transfers if:

8.1.1 based on the factors listed under paragraph 8.3 and 8.4, the transfer is necessary for data controller to carry out obligations in the contract; and

8.1.2 the obligations must be for the core purpose of the contract.

8.2 There must be a direct and objective link between the performance of contract and the cross border personal data transfers.

Necessity of the cross border transfer of personal data

8.3 The word 'necessary' contained in paragraph 129(3)(b), (c) and (g) of the Act 709 does not mean that the cross border personal data transfer has to be absolutely essential. However, the cross border personal data transfer must satisfy the following factors:

8.3.1 the cross border personal data transfer is not just practice or is carried out on a regular basis. The reasons for the transfer must be for the fulfilment of a specified purpose rather than for the general purposes or practices of the company;

Example:

A travel agency that intends to transfer personal data of its customer overseas may not rely on the argument that it is industry practice to transfer personal data out of Malaysia or that the purpose is for the travel agency's records or maintenance of its customer database.

On the other hand, the travel agency would be said to be transferring personal data out of Malaysia for a specified purpose if the transfer is for the purposes of booking accommodation or event tickets for its customers.

8.3.2 the cross border personal data transfer is made to achieve a specific purpose only and not for general purpose; and

Explanation:

A transfer is considered to be made to achieve a specific purpose if the data controller is able to prove that the transfer was carried out to fulfil certain purposes. These specific purposes must not purely be for the benefit of the data controller and should be specific to the data subject or small group of data subjects as opposed to all data subjects of the data controller.

8.3.3 data controller cannot reasonably achieve the specified purpose through any alternative means which can be feasibly carried out.

Explanation:

Data controller will be considered to have "feasible alternative means" if the alternative means are:

(a) able to be carried out at a lower or similar cost; and

(b) able to achieve similar results or outcomes.

For example, data controller who wishes to store personal data in a data centre outside Malaysia will be considered to have feasible alternative means if there are local data centres which offer data storage services at a lower or similar cost.

8.4 When making an assessment as to whether the cross border personal data transfer satisfies the above factors, data controller shall take into account the following:

8.4.1 the reason why the transfer is required;

8.4.2 the purposes for the transfer; and

8.4.3 whether there are any feasible alternatives available.

For the core purposes of the contract

8.5 The transfer of personal data must be directly related to and for the purposes of performing the obligations of the data controller as specified under the contract.

9. Transfer necessary for conclusion or performance of contract between data controller and third party

9.1 Data controller may refer to paragraph 129(3)(c) of the Act 709 for cross border personal data transfers if:

9.1.1 the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party;

9.1.2 the contract:

(a) is entered into at the request of the data subject; or

(b) is in the interests of the data subject;

9.1.3 based on the factors listed out under Paragraphs 8.3 and 8.4, the transfer is necessary for the conclusion or performance of the contract.

9.2 The request by the data subject referred to in paragraph 9.1.2(a) must be:

9.2.1 provided in written form; or

9.2.2 where the request was made through means other than in writing, the said request maintained and kept in a proper form that can be shown as proof that the data subject made such request.

9.3 Data controller that intends to refer to paragraph 9.1.2(b) (interests of data subject) may only do so if the interest of data subject is shown to be:

9.3.1 clear and substantial: there must be an obvious benefit which can be clearly identified and stated by the data controller;

9.3.2 direct: the benefit to the data subject arises as a direct result of the conclusion or performance of the contract; and

9.3.3 targeted towards the data subject: the primary aim or purpose of the contract shall provide direct benefits to the data subject.

Examples:

- Data subject buys a travel package for his family. The travel agency then enters into agreements with operators (such as hotel and flight operators) and subsequently transfers their personal data out of Malaysia to those operators for the purposes of making bookings related to the trip. This is considered a clear, direct and targeted benefit as the contract entered into:

(a) has a clear benefit. Data subject and his family will be able to go on holiday with their hotels and flights booked in advance;

(b) is direct. The performance of the contract between the travel agency and the operator provides direct benefits to the data subject and his family; and

(c) is targeted towards the data subject: the primary aim of the contract between the travel agency and operator is to ensure that the data subject and his family are able to go on holiday. It is also targeted towards the data subject and his family.

9.4 Additionally, data controller shall consider the factors listed under paragraphs 8.3 and 8.4 in relation to the conclusion or performance of the contract between the data controller and third party to ensure that the transfer is necessary.

10. Transfer for the purpose of legal proceedings

10.1 Data controller may refer to paragraph 129(3)(d) of the Act 709 for cross border personal data transfer if the transfer is for the purpose of:

10.1.1 legal proceedings;

10.1.2 obtaining legal advice; or

10.1.3 establishing, exercising or defending legal rights.

10.2 The legal proceeding includes the following:

10.2.1 a claim that would be brought and defended in a court (including civil and criminal law);

10.2.2 a claim that would be brought and defended in a tribunal (e.g. a consumer claims tribunal);

10.2.3 administrative or regulatory procedure (e.g. to defend an investigation (or potential investigation) in competition or financial services law, or to seek approval for a merger); or

10.2.4 an out-of-court procedure (e.g. without prejudice meeting, mediation or arbitration).

10.3 Data controller shall not refer to the condition under paragraph 129(3)(d) of the Act 709 if there is only a possibility that a legal proceeding or other formal proceedings may be brought in the future. Nevertheless, data controller may refer to this condition if the data controller:

10.3.1 is engaged in pre-action correspondence;

10.3.2 is taking advice about the legal risk in bringing or defending a claim; or

10.3.3 has received a request for information from an overseas regulatory authority with a view to it potentially taking formal action.

11. Reasonable grounds of the data controller

11.1 Data controller may refer to paragraph 129(3)(e) of the Act 709 for cross border personal data transfers if it has reasonable grounds for believing that:

11.1.1 the transfer is for the avoidance or mitigation of adverse action against the data subject;

11.1.2 it is not practicable to obtain the consent in writing of the data subject for that transfer; and

11.1.3 if it was practicable to obtain such consent, the data subject would have given his consent.

11.2 Paragraph 129(3)(e) of the Act 709 only applies if it is not possible for the data subject to give their consent such is:

11.2.1 data subject is unconscious;

11.2.2 data subject is not contactable and given the circumstances, reasonable and proportionate steps have been taken to try and contact them; or

11.2.3 data subject is unable to provide consent due to insufficient time for the provision of all the information needed for a consent.

12. Requirement to take all reasonable precautions and exercise all due diligence for cross border transfers of personal data

12.1 Data controller may refer to paragraph 129(3)(f) of the Act 709 for any cross border personal data transfer if the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the Act 709. In this regard, all reasonable precautions and exercised due diligence may be deciphered by the following mechanisms:

12.1.1 Binding Corporate Rules ("**BCR**");

12.1.2 Contractual Clauses ("**CC**"); or

12.1.3 Certification under an approved certification scheme ("**Certification**").

Binding Corporate Rules

12.2 BCR is personal data protection policies that are implemented by multinational corporate group, group of undertakings or a group of enterprise engaged in a

joint economic activity such as franchise, joint venture or professional partnership.

12.3 Data controller may refer to BCR that applies to the data controller and receiver for any cross border personal data transfer that are intra-group in nature.

Explanation:

Data Controller may carry out cross border personal data transfers to its franchisor or subsidiary company where there exists a BCR that is implemented by both the data controller and receiver.

12.4 The requirements for BCR are:

12.4.1 the BCR contains the following details:

(a) parties governed under BCR;

(b) specified countries/ jurisdictions where personal data may be transferred to;

(c) the legally binding nature of the BCR to all parties to the BCR and to any data subject of the parties to the BCR in relation to the data transfer made under the BCR;

(d) requirement for parties to ensure a standard of protection equivalent to the Act 709;

(e) requirement to comply with the personal data protection principles;

(f) personal data retention periods;

(g) reporting of any personal data breach;

(h) mechanisms for ensuring compliance;

(i) apportionment of liability for any personal data breach;

(j) requirements or restrictions related to the transfer of personal data to any third party service provider;

(k) the rights of data subject and methods to exercise their rights;

(l) the implementation of audit to ensure compliance by each party;

(m) effective date and last reviewed date of the BCR;

(n) responsibilities of the Data Protection Officer or any other person responsible for monitoring compliance with BCR; and

(o) complaint procedures.

12.4.2 BCR is legally binding on all parties to the contract and can be legally enforced; and

12.4.3 BCR is reviewed from time to time to ensure that it is up to date.

12.5 Any review of the BCR is to take into account the latest developments in the relevant data protection laws. The data controller is also encouraged to appoint an independent auditor to review the BCR to ensure that it is compliant with the Act 709.

Contractual Clauses

12.6 CC is a set of clauses inserted into a contract which would legally bind both the data controller and receiver to ensure adequate level of protection in relation to the processing of personal data.

12.7 Data controller who wishes to adhere to CC, shall ensure that the CC, at least, cover the following:

12.7.1 the security measures that are to be implemented to provide adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by Act 709; and

12.7.2 clauses that state and guarantee that the processing of personal data shall be carried out in compliance with the Act 709.

12.8 Data controller relying on the use of CC shall at all times take all reasonable precautions to ensure that the receiver complies with the terms provided by the CC. In the event that the data controller discovers a breach of terms provided by the CC, the data controller shall cease the transfer of personal data to the other parties to the contract until such party rectifies the breach.

Use of the International Model

12.9 Data controller who wishes to use the international model may adopt the following list of contractual clauses including, but not limited to:

12.9.1 the Association of Southeast Asian Nations (ASEAN) Model Contractual Clauses for Cross Border Data Flows;

12.9.2 the European Union General Data Protection Regulation (EU GDPR) Standard Contractual Clauses for the Transfer of Personal Data to Third Countries; or

12.9.3 such other CC as determined by the Commissioner from time to time.

12.10 Prior to the use of international model above, data controller is recommended to review the CC to determine whether any additional clauses are necessary to be included to ensure adequate level of protection which is at least equivalent to the level of protection afforded by Act 709.

Certification

12.11 Data controller/ data processor may obtain certification regarding personal data protection as a method of verifying that the data controller/ data processor has in place adequate policies and processes to comply with data protection standard/ laws or provide an adequate level of protection to protect personal data.

Example:

- Europrivacy is a certification scheme managed by the European Centre for Certification and Privacy and is designed to assess, document, certify and value compliance with the EU GDPR.

- The Legal Services Operational Privacy Certification Scheme is designed to assist legal service providers demonstrate compliance with United Kingdom data protection law when processing their clients' personal data.

- The Asia Pacific Economic Cooperation Cross Border Privacy Rules System ("APEC CBPR") and Privacy Recognition for Processors ("APEC PRP") Certification is issued by the Infocomm Media Development Authority (Singapore) and TrustArc to certify that the data protection policies and processes of data controller/ data processor complies with the APEC CBPR and APEC PRP Principles.

12.12 Data controller may refer to the condition under paragraph 129(3)(f) of the Act 709 to transfer personal data out of Malaysia if:

12.12.1 receiver possesses a valid Recognised Certificate;

12.12.2 data controller undertakes reasonable efforts to verify the validity of the Recognised Certificate;

Example:

Reasonable efforts to verify the validity of the Recognised Certificate include:

(a) obtaining a certified true copy of the Recognised Certificate; and

(b) where possible, verify the validity of the Recognised Certificate through an online database. For example, Europrivacy has a Registry of Certificates that allows members of the public to search for and verify the validity of the Recognised Certificate.

12.12.3 data controller enters into a contract with the receiver which:

(a) imposes an obligation on the receiver to ensure that it has in place adequate level of protection to protect personal data transferred to; and

(b) warrants that the Recognised Certificate is valid.

12.13 Data controller shall at all times take all reasonable precautions to ensure that the receiver complies with its obligations to protect personal data. In the event that the data controller discovers a breach of such obligations, the data controller shall cease the transfer of personal data to the receiver until the breach has been rectified.

13. Transfer necessary to protect the vital interests of the data subject

Vital Interests of data subject

13.1 Data controller may refer to paragraph 129(3)(g) of the Act 709 for any cross border personal data transfer if:

13.1.1 the necessity of the transfer satisfies the factors laid out under paragraph 8.3 and 8.4; and

13.1.2 the purpose of the cross border personal data transfer is to protect the vital interests of the data subject.

13.2 Notwithstanding paragraph 13, the risk to the data subject's vital interests must outweigh any personal data protection concerns.

Example:

Data controller may refer to paragraph 129(3)(g) of the Act 709, for cross border personal data transfer if a Malaysian Data Subject is in a coma in Singapore and personal data about his/ her medical history needs to be transferred to Singapore for his/ her essential medical treatment.

If the Malaysian Data Subject is conscious and capable of giving consent, and the data controller has sufficient time to obtain consent, cross border personal data transfer does not fulfil the requirement under paragraph 129(3)(g) Act 709.

PART C: HANDLING CROSS BORDER PERSONAL DATA TRANSFER

14. Responsibilities of the data controller when transferring personal data

14.1 Data controller is responsible for the security of personal data when transferring out of Malaysia and shall take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

14.2 Data controller shall ensure that the method for transferring personal data out of Malaysia is secure and in line with the Security Principle under the Act 709, subsidiary legislation, standard and any other applicable guidelines relating to protection of personal data.

15. Dealing with third party/ data processor

15.1 Data controller shall ensure that any contract entered into with third party/ data processor contains clauses governing the processing of personal data, including the security of personal data.

15.2 Data controller shall ensure that data processor complies with Section 9 of the Act 709, subsidiary legislation, standard and any other applicable guidelines relating to protection of personal data.

16. Record keeping

16.1 Data controller that carries out cross border transfer of personal data must keep and maintain record of the receiver to whom the personal data is transferred to. Such record shall contain the following details:

16.1.1 the details of the receiver at least the following:

(a) the name of the receiver;

(b) company registration number (if any); and

(c) contact details of the Data Protection Officer or such other person at the receiver's end;

16.1.2 the country that the personal data is being transferred to;

16.1.3 the type of personal data transferred;

16.1.4 purposes of the transfer; and

16.1.5 such other information as the data controller deems necessary.

16.2 Additionally, data controller that carries out cross border personal data transfer must keep and maintain record that may sufficiently prove that each cross border personal data transfer complies with Section 129 of the Act 709. Examples of such records include:

Conditions	Record
Subsection 129(2) of the Act 709	- Record of TIA; and - Findings of TIA.
Paragraph 129(3)(a) of the Act 709	- Personal data protection notice; and - Record of data subject's consent.
Necessary for the performance of a contract	- Copy of the contract; and - Proof that the processing is necessary for the performance of the contract.
Reasonable precautions and due diligence	- Copy of BCR; - Copy of the Recognised Certificate; or - Copy of the signed contract between data controller and receiver.

16.3 Data controller must keep and maintain records provided under paragraph 16.1 subject to Retention Principle under the Act 709, subsidiary legislation, standard and any other applicable guidelines relating to protection of personal data or other laws in force.