KERTAS KONSULTASI AWAM BIL. 1/2026 :

KERANGKA KECERDASAN BUATAN (AI) DAN PERLINDUNGAN DATA PERIBADI

Tarikh Mula : 5 Oktober 2026

Tarikh Akhir : 23 Oktober 2026

BAHAGIAN 1 : PENGENALAN DAN LATAR BELAKANG

1. Pengenalan

1.1. Kertas Konsultasi Awam ini dikeluarkan oleh Jabatan Perlindungan Data Peribadi (JPDP) bagi mendapatkan maklum balas, pandangan dan cadangan daripada pemegang taruh, pengawal data, pemproses data, wakil industri serta orang awam berhubung cadangan pembangunan **Kerangka Kecerdasan Buatan (AI) dan Perlindungan Data Peribadi** ("**Kerangka**") di bawah **Akta Perlindungan Data Peribadi 2010** ***[Akta 709]***.

1.2. Kerangka ini dicadangkan sebagai dokumen rujukan utama untuk:

1.2.1. **Memperjelas Tanggungjawab Kawal Selia:** Menjelaskan peranan serta obligasi pengawal data dan pemproses data di bawah Akta 709 apabila memproses data peribadi melalui sistem AI.

1.2.2. **Menggariskan Amalan Terbaik:** Menyediakan langkah praktikal berhubung pemprosesan data peribadi merentasi pelbagai model AI, sama ada yang dibangunkan secara dalaman (*in-house*), diperoleh daripada pihak ketiga (*off-the-shelf*), disesuaikan (*bespoke*) atau dibenamkan (*embedded*) ke dalam platform, aplikasi dan perkhidmatan digital (SaaS/API).

1.2.3. **Memperkukuh Tadbir Urus Data:** Meningkatkan akauntabiliti, ketelusan, keselamatan teknikal, pengurusan risiko dan perlindungan hak subjek data sepanjang kitaran hayat sistem AI.

1.3. JPDP mengalu-alukan maklum balas daripada semua pihak bagi memastikan Kerangka ini bersifat praktikal, seimbang dan berupaya menyokong inovasi digital tanpa mengabaikan Hak Subjek Data serta Prinsip-Prinsip Perlindungan Data Peribadi di bawah Akta 709.

2. Latar Belakang dan Penyataan Masalah

2.1. Latar Belakang Perundangan & Perkembangan Teknologi

2.1.1. Akta 709 menyediakan kerangka perundangan utama bagi melindungi data peribadi dan mengawal selia pemprosesan data peribadi dalam transaksi komersial di Malaysia. Akta

ini menjadi teras penting dalam membina kepercayaan terhadap ekosistem digital secara bertanggungjawab, telus, selamat dan beretika.

2.1.2. Perkembangan pesat teknologi AI, automasi, analitik data, Internet Benda (IoT), pengkomputeran awan serta Model AI Tujuan Umum (*General-Purpose AI Models*) telah meningkatkan penggunaan data peribadi merentasi pelbagai sektor. Walaupun perkembangan ini membuka ruang inovasi dan peningkatan kecekapan produktiviti, ia turut menimbulkan cabaran baharu berhubung kerahsiaan, keselamatan data, pemprofilan, pembuatan keputusan automatik dan pematuhan prinsip privasi.

2.2. Penandaarasan Antarabangsa (*International Benchmarking*)

2.2.1. Bagi memastikan Kerangka ini selari dengan piawaian serta amalan terbaik global, JPDP telah mengambil kira perkembangan pengawalseliaan antarabangsa daripada pelbagai bidang kuasa dan pertubuhan global. Penandaarasan ini merangkumi perundangan AI oleh Kesatuan Eropah (EU) dan prinsip tadbir urus AI daripada OECD (Organisation for Economic Co-operation and Development). Di samping itu, Kerangka ini turut meneliti pelbagai garis panduan, kerangka perlindungan data peribadi serta khidmat nasihat berhubung persekitaran AI yang dikeluarkan oleh Pihak Berkuasa Perlindungan Data Peribadi luar negara, antaranya Filipina (NPC), Hong Kong (PCPD), Singapura (PDPC) dan United Kingdom (ICO).

2.2.2. Pendekatan antarabangsa ini menyediakan penandaarasan penting dalam pembangunan Kerangka yang berkadar dengan tahap risiko, melindungi data peribadi dan memupuk pembangunan serta penggunaan AI secara bertanggungjawab.

2.3. Penyataan Masalah (*Problem Statement*)

2.3.1. Data peribadi diproses merentasi keseluruhan kitaran hayat sistem AI iaitu daripada perancangan, rekabentuk, penyediaan data latihan, pengujian, pelaksanaan, pengoperasian, pemantauan hinggalah penamatan sistem. Panduan tadbir urus yang tidak jelas boleh menimbulkan pelbagai risiko seperti berikut:

i. **Risiko Etika & Bias:** Keputusan yang dihasilkan oleh sistem AI berisiko menjadi tidak adil, semberono atau bersifat diskriminasi (*algorithmic bias*).

ii. **Pencerobohan Privasi & Kebocoran Data:** Skop pengumpulan data latihan berisiko menjadi tidak jelas, di samping berlakunya ketidakpatuhan terhadap kawalan akses serta penyulitan data.

iii. **Ketidaktelusan Keputusan Automatik:** Keputusan dipacu AI yang sukar dijelaskan (*opaque decision-making*) boleh menjejaskan hak subjek data di bawah Akta 709.

2.3.2. Sehubungan itu, Kerangka ini dicadangkan bagi memperkukuh tadbir urus dan pengurusan risiko dalam ekosistem AI agar pemprosesan data peribadi dilaksanakan secara sah, telus, selamat dan bertanggungjawab.

BAHAGIAN 2 : RINGKASAN KERANGKA KECERDASAN BUATAN (AI) DAN PERLINDUNGAN DATA PERIBADI

3.1. Kerangka yang dicadangkan merangkumi 10 bahagian utama (**Bahagian A** hingga **Bahagian J**) yang disusun mengikut kitaran hayat sistem AI seperti jadual berikut:

Bil.	Bahagian	Ringkasan Skop & Kawalan
1.	Bahagian A: Pengenalan	Menjelaskan latar belakang, tujuan dan skop pemakaian Kerangka di bawah Akta 709 bagi pemprosesan data peribadi menerusi sistem AI.
2.	Bahagian B: Tafsiran & Konsep Utama	Menjelaskan tafsiran dan konsep teknikal AI yang digunakan dalam Kerangka.
3.	Bahagian C: Asas Perundangan	Menggariskan asas perundangan termasuk pengecualian dalam pemprosesan data peribadi menerusi sistem AI.
4.	Bahagian D: Pembangunan & Pengujian	Menetapkan piawaian pengumpulan dataset latihan serta keperluan pengujian dan pengesahan model sebelum AI dilaksanakan.

Bil.	Bahagian	Ringkasan Skop & Kawalan
5.	Bahagian E: Pelaksanaan & Pengoperasian	Mengawal penyeliaan fasa pengoperasian, pemantauan prestasi berterusan, latihan semula model hingga penamatan sistem secara selamat.
6.	Bahagian F: Perolehan & AI Luaran	Usaha wajar (*due diligence*) terhadap penyedia AI luaran, perjanjian pemprosesan data dan pemindahan data rentas sempadan.
7.	Bahagian G: Hak Subjek Data	Menggariskan perlindungan dan mekanisme bagi membolehkan subjek data melaksanakan hak mereka di bawah Akta 709.
8.	Bahagian H: Langkah Perlindungan & Kesaksamaan	Menggariskan kawalan keselamatan teknikal, integriti data, pengurusan insiden pelanggaran data dan pencegahan keputusan AI yang bias/berat sebelah.
9.	Bahagian I: Tadbir Urus & Pengurusan Risiko	Menggariskan struktur pengawasan organisasi, penilaian risiko serta keperluan ketelusan dan kebolehjelasan (*explainability*) keputusan AI.
10.	Bahagian J: Dokumentasi & Audit	Penyelenggaraan rekod pematuhan kitaran hayat AI, semakan audit berkala dan pembuktian pematuhan kepada Pesuruhjaya.

3.2. Draf penuh Kerangka adalah seperti yang dinyatakan dalam **Lampiran 1.**

BAHAGIAN 3 : SOALAN KONSULTASI AWAM

4.1. JPDP mengalu-alukan maklum balas secara tertulis berasaskan soalan-soalan berikut:

4.1.1. **Kecukupan Pematuhan Akta 709**
Adakah Kerangka yang dicadangkan ini memadai untuk menyokong pematuhan terhadap Akta 709 dalam pembangunan dan penggunaan sistem AI yang melibatkan pemprosesan data peribadi? Jika tidak, sila nyatakan aspek yang perlu ditambah baik atau diperjelas.

4.1.2. **Skop, Terma & Pengecualian**
Selain skop dan takrifan yang dicadangkan (seperti Sistem AI, Model AI Tujuan Umum, Penyahnamaan, Penyamaran), adakah terdapat konsep, keadaan, batasan atau pengecualian tambahan yang perlu dipertimbangkan? Sila nyatakan cadangan berserta justifikasi dan contoh kes penggunaan (*use case*).

4.1.3. **Prinsip Kitaran Hayat AI**
Adakah pendekatan yang dicadangkan memadai untuk memastikan data peribadi diproses secara sah, adil, telus, selamat dan bertanggungjawab sepanjang kitaran hayat sistem AI? Sila kemukakan cadangan khusus untuk menambah baik prinsip, langkah kawalan atau amalan terbaik yang dicadangkan.

4.1.4. **Tadbir Urus & Kebolehkelaksanaan (*Feasibility*)**
Adakah keperluan tadbir urus, langkah perlindungan, pengurusan risiko dan akauntabiliti yang dicadangkan jelas, praktikal serta berkadar (*proportionate*) dengan tahap risiko, peranan dan keupayaan organisasi? Sila nyatakan penambahbaikan yang diperlukan.

4.1.5. **Kekangan & Cabaran Penguatkuasaan**
Apakah kekangan atau cabaran utama yang mungkin dihadapi oleh organisasi sekiranya keperluan dalam Kerangka ini dikuatkuasakan di bawah Akta 709? Sila nyatakan cadangan langkah mitigasi bagi menangani kekangan tersebut.

4.1.6. **Persediaan Industri & Sokongan Kawal Selia**
Apakah persediaan yang diperlukan oleh pihak berkepentingan sebelum keperluan dalam Kerangka ini dilaksanakan atau dikuatkuasakan? Sila nyatakan persediaan utama serta bentuk sokongan kawal selia (seperti garis panduan tambahan, tempoh peralihan atau *sandbox*) yang diperlukan.

4.1.7. **Rujukan & Standard Antarabangsa**
Apakah undang-undang, standard, garis panduan, kerangka kerja, atau pendekatan pengawalseliaan di peringkat tempatan atau antarabangsa yang wajar dijadikan rujukan bagi memperkukuh Kerangka ini? Sila nyatakan dokumen dan aspek yang berkaitan.

BAHAGIAN 4 : TATACARA MENGEMUKAKAN MAKLUM BALAS

5.1. Penyerahan maklum balas dan cadangan berhubung Kerangka ini hendaklah dikemukakan **sebelum atau pada 23 Oktober 2026** melalui platform dalam talian rasmi seperti berikut:

5.1.1. **Platform Atas Talian (UPC)**: https://upc.mpc.gov.my/view-consultation/296; atau

5.1.2. **Google Form Rasmi**: https://forms.gle/GKfBZXgGZUevgWa79

5.2. Sila imbas Kod QR di bawah untuk mengakses platform dalam talian rasmi:

5.3. Untuk sebarang pertanyaan, penjelasan atau maklumat lanjut berkenaan Kertas Konsultasi Awam ini, sila hubungi saluran berikut:

E-mel Rasmi: risiko@pdp.gov.my

No. Telefon: +603-2021 1183/ 1184/ 1185

Alamat Surat-Menyurat:
Jabatan Perlindungan Data Peribadi
Aras 8, Galeria PjH. Jalan P4W
Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya, Malaysia.

GARIS PANDUAN PERLINDUNGAN DATA PERIBADI

Kerangka Kecerdasan Buatan (AI) dan Perlindungan Data Peribadi

Versi 1.0

Tarikh Terbitan: **XX XX XXXX**

ISI KANDUNGAN

BAHAGIAN A: PENGENALAN 3

1. Latar Belakang 3
2. Peruntukan Undang-Undang 4

BAHAGIAN B: PENGENALAN KEPADA TAFSIRAN DAN KONSEP UTAMA 4

3. Tafsiran 4
4. Konsep Khusus AI 6

BAHAGIAN C: ASAS UNDANG-UNDANG BAGI PENGGUNAAN DATA PERIBADI DALAM SISTEM AI 7

5. Asas Undang-Undang bagi Penggunaan Data Peribadi dalam Sistem AI 7
6. Pengumpulan dan Penggunaan Data Peribadi yang Sah 7
7. Notis kepada Subjek Data 7
8. Pemprosesan Berasaskan Persetujuan 8
9. Pemprosesan Data Peribadi Sensitif 9
10. Pemprosesan Tanpa Persetujuan dan Pengecualian 9

BAHAGIAN D: PEMBANGUNAN DAN PENGUJIAN SISTEM AI 10

11. Keperluan Am bagi Pembangunan Sistem AI 10
12. Pengumpulan dan Penyediaan Data bagi Pembangunan AI 10
13. Pembangunan Sistem AI 11
14. Pengujian dan Pengesahan Sebelum Pelaksanaan 11

BAHAGIAN E: PELAKSANAAN DAN PENGGUNAAN SISTEM AI DALAM PEMPROSESAN DATA PERIBADI 12

15. Pelaksanaan Sistem AI 12
16. Penggunaan Sistem AI dalam Pemprosesan Data Peribadi 12
17. Pemantauan Operasi 13
18. Pengubahsuaian, Latihan Semula dan Penggunaan Berterusan 13
19. Penamatan dan Pelucutan Operasi Sistem AI 14

BAHAGIAN F: PEROLEHAN, INTEGRASI DAN PENGURUSAN SISTEM AI LUARAN ... 14

20. Pengurusan Sistem AI Luaran dan Penyedia Perkhidmatan 14
21. Peranan, Tanggungjawab dan Sempadan Pemprosesan Data 15
22. Pemprosesan dan Pemindahan Data Peribadi Rentas Sempadan 16
23. Pengawasan Berterusan Sistem AI Luaran 16

BAHAGIAN G: HAK SUBJEK DATA DALAM SISTEM AI 17

24. Hak Subjek Data dalam Sistem AI 17
25. Hak untuk Mengakses Data Peribadi 17

26. Hak untuk Membetulkan Data Peribadi 17
27. Hak untuk Menarik Balik Persetujuan 17
28. Hak kepada Kemudahalihan Data 17
29. Memudahkan Pelaksanaan Hak Subjek Data 18
BAHAGIAN H: LANGKAH PERLINDUNGAN UTAMA DAN OBLIGASI KESAKSAMAAN DALAM SISTEM AI 18
30. Langkah Perlindungan Utama dan Obligasi Kesaksamaan dalam Sistem AI 18
31. Kesaksamaan dan Pencegahan Hasil yang Tidak Adil 18
32. Langkah Perlindungan Keselamatan 19
33. Insiden Keselamatan dan Pelanggaran Data Peribadi 20
34. Ketepatan dan Integriti Data 20
BAHAGIAN I: TADBIR URUS DAN PENGURUSAN RISIKO 21
35. Tadbir Urus dan Pengawasan Organisasi 21
36. Polisi, Prosedur dan Kesedaran 21
37. Pengurusan Risiko 21
38. Ketelusan dan Kebolehjelasan 23
39. Semakan Dalaman, Pembuktian Pematuhan dan Pengawasan Berterusan 23
BAHAGIAN J: DOKUMENTASI, AUDIT DAN PEMATUHAN 24
40. Dokumentasi dan Penyimpanan Rekod 24
41. Semakan Dalaman dan Audit 24
42. Pembuktian Pematuhan 25
43. Pengawasan Berterusan 26

BAHAGIAN A: PENGENALAN

1. Latar Belakang

1.1 Akta Perlindungan Data Peribadi 2010 ("**Akta 709**") menetapkan kerangka perundangan bagi melindungi data peribadi di Malaysia, termasuk Prinsip-Prinsip Perlindungan Data Peribadi ("Prinsip") yang mengawal selia pemprosesan data peribadi.

1.2 Kerangka Kecerdasan Buatan (AI) dan Perlindungan Data Peribadi ("**Kerangka**") ini dibangunkan bagi membantu pengawal data memahami dan mengaplikasikan kehendak Akta 709 apabila data peribadi diproses melalui sistem AI. Ini termasuk sistem AI yang dibangunkan secara dalaman, diperoleh daripada pemaju atau vendor luar atau diintegrasikan ke dalam penyelesaian digital yang lebih luas. Mengikut kesesuaian, Kerangka ini turut menyediakan panduan kepada pemproses data berhubung dengan obligasi mereka di bawah Prinsip Keselamatan.

1.3 Seiring dengan peningkatan penggunaan sistem AI bagi penyampaian perkhidmatan, menyokong operasi organisasi dan mengautomasikan proses membuat keputusan, Kerangka ini bertujuan untuk:

(a) menyokong pematuhan kepada Akta 709;

(b) menjelaskan bagaimana data peribadi boleh diproses melalui sistem AI selaras dengan Akta 709;

(c) menggalakkan amalan AI yang bertanggungjawab dan boleh dipercayai (*trustworthy*) dalam pemprosesan data peribadi;

(d) menggalakkan penerapan langkah-langkah tadbir urus, kebertanggungjawaban dan pengurusan risiko yang bersesuaian sepanjang kitaran hayat sistem AI; dan

(e) memupuk kepercayaan dan keyakinan orang awam terhadap produk serta perkhidmatan yang didorong oleh AI.

1.4 Melainkan jika konteks menghendaki sebaliknya, rujukan kepada pengawal data dalam Kerangka ini hendaklah terpakai, jika berkenaan, kepada pemproses data atau pihak ketiga di bawah Akta 709, apabila mana-mana entiti:

(a) memperoleh atau mendapatkan penyelesaian, produk, sistem, atau perkhidmatan AI daripada pembangun, vendor atau penyedia perkhidmatan pihak ketiga yang melibatkan pemprosesan data peribadi;

(b) membangunkan, melaksanakan (*deploy*) atau menyesuaikan (*customise*) penyelesaian, produk, sistem, atau perkhidmatan AI yang memproses data peribadi bagi domain atau kes penggunaan *(use case)* yang spesifik; atau

(c) menyediakan, menyokong atau mengendalikan penyelesaian, produk, sistem, atau perkhidmatan AI yang memproses data peribadi dalam penyampaian perkhidmatan atau menyokong operasi perniagaan, termasuk di mana penyedia sistem AI tersebut mempunyai akses kepada data peribadi tersebut.

1.5 Kerangka ini terpakai kepada pemprosesan data peribadi melalui atau berkaitan dengan sistem AI, tanpa mengira sama ada sistem AI tersebut:

(a) dibangunkan secara dalaman, termasuk penyelesaian AI yang dibangunkan khusus *(bespoke)* atau bersifat proprietari;

(b) diperoleh daripada pembangun atau vendor pihak ketiga, termasuk sistem AI sedia guna *(off-the-shelf)*, tersuai atau sumber terbuka; atau

(c) dibenamkan (*embedded*) dalam platform atau perkhidmatan digital yang lebih luas, termasuk Perisian-sebagai-Perkhidmatan (SaaS), perkhidmatan berasaskan awan, Antara Muka Pengaturcaraan Aplikasi (API) atau teknologi lain yang dipacu oleh AI.

1.6 Kerangka ini juga terpakai apabila model AI tujuan umum (*general-purpose AI models*) digabungkan ke dalam aplikasi, perkhidmatan atau persekitaran operasi khusus yang memproses data peribadi.

1.7 Kerangka ini melengkapi dan hendaklah dibaca bersama-sama dengan Akta 709 serta mana-mana instrumen perundangan lain yang relevan yang dikeluarkan di bawah Akta 709. Tiada apa-apa dalam Kerangka ini boleh ditafsirkan sebagai mengehadkan, menggantikan atau mengubah apa-apa obligasi yang dikenakan di bawah Akta 709 atau mana-mana undang-undang bertulis lain yang terpakai.

1.8 Kerangka ini disusun berdasarkan kitaran hayat sistem AI. Kerangka ini menggariskan amalan terbaik peringkat tertinggi serta langkah-langkah praktikal bagi menyokong tadbir urus AI yang bertanggungjawab dan pematuhan kepada Akta 709 sepanjang peringkat perancangan, pembangunan, perolehan, pelaksanaan, pengoperasian, pemantauan dan penamatan sistem AI.

1.9 Kerangka ini boleh disemak dan dipinda oleh Pesuruhjaya Perlindungan Data Peribadi ("**Pesuruhjaya**") dari semasa ke semasa bagi mengambil kira perkembangan undang-undang, teknologi, amalan kawal selia dan tadbir urus AI.

2. Peruntukan Undang-Undang

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

BAHAGIAN B: PENGENALAN KEPADA TAFSIRAN DAN KONSEP UTAMA

3. Tafsiran

3.1 Melainkan jika ditakrifkan sebaliknya dalam Kerangka ini, istilah dan ungkapan yang digunakan dalam Kerangka ini hendaklah mempunyai makna yang sama sebagaimana yang ditetapkan di bawah Akta 709 dan mana-mana instrumen perundangan berkaitan yang dikeluarkan di bawah Akta 709.

3.2 Dalam Kerangka ini, melainkan jika konteksnya menghendaki maksud yang lain:

"Sistem AI"	ertinya sistem berasaskan mesin yang direka bentuk untuk beroperasi dengan tahap autonomi yang berbeza-beza dan yang boleh menunjukkan keupayaan adaptasi selepas pelaksanaan. Sistem

	tersebut memproses input untuk melaksanakan tugas dengan mempelajari daripada data dan/atau membuat inferens daripada corak bagi menghasilkan output seperti ramalan, syor, kandungan atau keputusan yang boleh mempengaruhi persekitaran fizikal atau maya.
"Penyedia Perkhidmatan AI"	ertinya mana-mana orang atau organisasi selain pengawal data yang membangunkan, menyediakan, mengehos, mengendalikan, menyelenggara atau selainnya menyokong sistem, model, fungsi atau perkhidmatan AI untuk digunakan oleh pengawal data.
"Penyahnamaan"	ertinya proses memproses data peribadi secara tidak boleh berbalik sedemikian rupa sehingga subjek data tidak lagi boleh dikenal pasti secara langsung atau tidak langsung dengan mengambil kira risiko pengenalpastian semula.
"Penyahkenalpastian"	ertinya proses membuang, mengubah suai, mengaburkan atau mentransformasikan pengenal pasti peribadi seperti nama, nombor kad pengenalan atau alamat daripada set data supaya subjek data tidak lagi boleh dikenal pasti secara langsung.
"Sistem AI Luaran"	ertinya sistem, model, fungsi atau perkhidmatan AI yang dibangunkan, disediakan, diintegrasikan, dihoskan, dikendalikan, diselenggara atau selainnya disediakan oleh Penyedia Perkhidmatan AI dan diperoleh, diintegrasikan atau digunakan oleh pengawal data berhubung dengan pemprosesan data peribadi.
"Model AI tujuan umum"	ertinya model AI yang direka bentuk untuk melaksanakan atau menyokong pelbagai tugas merentasi aplikasi atau domain yang berbeza dan tidak terhad kepada satu fungsi khusus.
"Sistem AI Tujuan Umum"	ertinya sistem AI yang menggabungkan model AI tujuan umum dan berupaya menyokong pelbagai tugas atau aplikasi, termasuk melalui penggunaan secara terus atau integrasi ke dalam sistem AI, aplikasi, produk atau perkhidmatan yang lain.
"Penyamaran"	ertinya pemprosesan data peribadi sedemikian rupa sehingga data peribadi tersebut tidak lagi boleh dikaitkan dengan subjek data yang khusus tanpa menggunakan maklumat tambahan, dengan syarat maklumat tambahan tersebut disimpan secara berasingan dan tertakluk kepada langkah teknikal dan organisasi yang bersesuaian.

"Pengenalpastian semula"	ertinya proses mengenal pasti subjek data daripada data yang sebelum ini telah dinyahkenalpasti atau disamar, termasuk dengan menghubungkan atau menggabungkan data tersebut dengan maklumat tambahan.

4. Konsep Khusus AI

Sistem AI

4.1 Sistem AI boleh menggunakan perisian, algoritma, model pembelajaran mesin, peraturan pra-takrif atau kaedah pengkomputeran lain, secara berasingan atau gabungan dalam melaksanakan fungsinya.

Model AI Tujuan Umum

4.2 Model AI tujuan umum boleh termasuk, sebagai contoh, Model Bahasa Besar *(Large Language Models)* ("**LLMs**") dan model asas *(foundation models)* yang menyokong fungsi seperti pemprosesan bahasa semula jadi, aplikasi perbualan, penjanaan kandungan, analisis imej atau tugas tujuan umum yang lain.

4.3 Model AI tujuan umum boleh disepadukan ke dalam atau menjadi sebahagian daripada satu atau lebih sistem AI, aplikasi, produk, perkhidmatan atau persekitaran operasi.

Sistem AI Tujuan Umum

4.4 Sistem AI tujuan umum boleh disesuaikan, dikonfigurasikan atau digunakan bagi maksud, aplikasi atau konteks operasi tertentu dengan memanfaatkan keupayaan yang lebih luas daripada model AI tujuan umum yang mendasarinya.

Penyahkenalpastian

4.5 Penyahkenalpastian merupakan konsep umum yang merangkumi pelbagai teknik (termasuk penyamaran *(pseudonymisation)* dan penyahnamaan *(anonymisation)*) yang mewakili tahap perlindungan yang berbeza merentasi spektrum kebolehkenalpastian data.

Penyahnamaan

4.6 Penyahnamaan boleh melibatkan teknik seperti pengagregatan (*aggregation*), pengguguran (*suppression*), pengitlakan (*generalisation*) atau penyamaran (*masking*), dengan syarat data yang dihasilkan tidak membolehkan subjek data dikenal pasti atau dikenali pasti semula secara munasabah.

Penyamaran

4.7 Penyamaran boleh termasuk, sebagai contoh, menggantikan pengenal pasti langsung seperti nama atau nombor kad pengenalan dengan kod, token atau pengenal pasti samaran lain, sambil mengekalkan maklumat tambahan yang membolehkan data tersebut dikaitkan semula dengan subjek data.

4.8 Data yang disamar masih boleh menimbulkan risiko pengenalpastian semula, khususnya melalui penggunaan maklumat tambahan atau apabila digabungkan

dengan maklumat yang tersedia secara awam atau sumber data lain.

BAHAGIAN C: ASAS UNDANG-UNDANG BAGI PENGGUNAAN DATA PERIBADI DALAM SISTEM AI

5. Asas Undang-Undang bagi Penggunaan Data Peribadi dalam Sistem AI

5.1 Penggunaan sistem AI tidak mewujudkan asas undang-undang yang berasingan bagi pemprosesan data peribadi. Sebarang pemprosesan data peribadi melalui sistem AI hendaklah mematuhi Akta 709, termasuk Prinsip-Prinsip Perlindungan Data Peribadi.

5.2 Pengawal data hendaklah memastikan pematuhan terhadap Akta 709 sepanjang kitaran hayat sistem AI termasuk pada peringkat perancangan, reka bentuk, pembangunan, pengujian, perolehan, pelaksanaan, pengintegrasian, pengoperasian, pemantauan, penyelenggaraan dan penamatan sistem AI.

5.3 Keperluan di bawah Akta 709 termasuk Prinsip-Prinsip Perlindungan Data Peribadi hendaklah terpakai di sepanjang kitaran hayat data peribadi, termasuk pengumpulan, penggunaan, penzahiran, penyimpanan dan pelupusan data peribadi yang diproses melalui sistem AI.

5.4 Penggunaan sistem AI tidak boleh mengurangkan atau menjejaskan hak subjek data di bawah Akta 709.

6. Pengumpulan dan Penggunaan Data Peribadi yang Sah

6.1 Sebelum memproses data peribadi melalui sistem AI, pengawal data hendaklah mengenal pasti tujuan pemprosesan dan menentukan asas undang-undang yang terpakai di bawah Akta 709. Pemprosesan tersebut hendaklah bagi maksud yang sah yang berhubung secara langsung dengan aktiviti pengawal data, dan data peribadi yang diproses hendaklah perlu, mencukupi dan tidak berlebihan berhubung dengan maksud tersebut.

6.2 Pengawal data kekal bertanggungjawab untuk memastikan bahawa pemprosesan data peribadi melalui sistem AI dilaksanakan secara sah dan selaras dengan Akta 709.

6.3 Sekiranya data peribadi diperoleh daripada sumber pihak ketiga, sumber yang tersedia secara awam atau set data luaran bagi pemprosesan berkaitan AI, pengawal data kekal bertanggungjawab untuk memastikan bahawa pengumpulan dan pemprosesan selanjutnya mematuhi Akta 709 serta kekal selaras dengan maksud asal data peribadi tersebut dikumpulkan atau disediakan.

7. Notis kepada Subjek Data

7.1 Sebelum atau pada masa data peribadi dikumpulkan untuk diproses melalui sistem AI, pengawal data hendaklah memberikan kepada subjek data suatu notis bertulis yang jelas dan mudah diakses, selaras dengan Prinsip Notis dan Pilihan di bawah Seksyen 7 Akta 709.

7.2 Notis bertulis tersebut hendaklah mengandungi maklumat yang dikehendaki di bawah Akta 709, termasuk data peribadi yang diproses, tujuan pemprosesan, apa-apa penggunaan sistem AI yang dimaksudkan jika berkenaan, golongan pihak ketiga

yang kepadanya data peribadi boleh dizahirkan, serta hak dan pilihan yang tersedia kepada subjek data.

7.3 Jika berkenaan, notis bertulis tersebut hendaklah memberikan maklumat yang mencukupi mengenai penggunaan sistem AI, termasuk sama ada sistem AI membuat atau menyokong keputusan yang memberi kesan kepada subjek data, menghasilkan syor atau ramalan, atau menyediakan output atau perkhidmatan yang diperibadikan dengan menggunakan data peribadi subjek data.

7.4 Sekiranya pengawal data bercadang untuk memproses data peribadi melalui sistem AI bagi tujuan yang tidak dinyatakan sebelum ini dalam notis bertulis, pengawal data hendaklah memberikan notis bertulis yang baharu atau dipinda kepada subjek data sebelum memulakan pemprosesan tersebut. Sekiranya persetujuan diperlukan di bawah Akta 709, persetujuan baharu juga hendaklah diperoleh.

Contoh:

Seorang pengguna memasang aplikasi kecergasan yang menggunakan AI untuk memberikan syor senaman yang diperibadikan. Sebelum mengumpulkan data peribadi pengguna, aplikasi tersebut memaparkan notis seperti berikut:

"Kami mengumpul dan memproses nama, umur dan pilihan kecergasan anda untuk menghasilkan syor senaman yang diperibadikan menggunakan AI. Data peribadi anda juga boleh dikongsi dengan penyedia perkhidmatan awan kami bagi tujuan tersebut. Sila rujuk Notis Perlindungan Data Peribadi kami untuk maklumat lanjut mengenai cara kami memproses data peribadi anda dan hak yang tersedia kepada anda."

8. Pemprosesan Berasaskan Persetujuan

8.1 Tertakluk kepada Akta 709, pengawal data tidak boleh memproses data peribadi, termasuk melalui sistem AI, melainkan subjek data telah memberikan persetujuan terhadap pemprosesan tersebut atau pemprosesan tersebut selainnya dibenarkan di bawah Akta 709.

8.2 Sekiranya persetujuan diperlukan di bawah Akta 709, pengawal data hendaklah memperoleh persetujuan subjek data bagi pemprosesan data peribadi, termasuk apabila pemprosesan tersebut dijalankan melalui sistem AI.

8.3 Sekiranya data peribadi diproses berasaskan persetujuan, pengawal data hendaklah memastikan bahawa:

(a) subjek data diberikan notis bertulis yang bersesuaian selaras dengan Akta 709;

(b) pemprosesan kekal dalam skop tujuan yang telah dimaklumkan kepada dan dipersetujui oleh subjek data;

(c) jika berkaitan, penggunaan sistem AI dalam pemprosesan data peribadi dimaklumkan dengan secukupnya kepada subjek data; dan

(d) persetujuan baharu diperoleh sekiranya tujuan pemprosesan yang dimaksudkan berbeza secara material daripada tujuan yang asal dipersetujui oleh subjek data, melainkan pemprosesan tersebut dibenarkan di bawah Akta 709.

8.4 Sekiranya subjek data berumur di bawah lapan belas (18) tahun atau tidak berupaya menguruskan hal ehwalnya sendiri, persetujuan hendaklah diperoleh daripada orang yang diberi kuasa di bawah Akta 709 untuk memberikan persetujuan bagi pihak subjek data.

8.5 Sekiranya subjek data menarik balik persetujuan dan meminta pengawal data menghentikan pemprosesan data peribadi tersebut, pengawal data hendaklah menghentikan pemprosesan data peribadi itu, termasuk pemprosesan melalui sistem AI dan mengambil langkah yang bersesuaian untuk memadamkan data peribadi tersebut apabila data itu tidak lagi diperlukan, melainkan pemprosesan atau penyimpanan berterusan selainnya dibenarkan di bawah Akta 709 atau mana-mana undang-undang bertulis yang lain.

9. Pemprosesan Data Peribadi Sensitif

9.1 Sekiranya data peribadi sensitif diproses, termasuk melalui sistem AI, pengawal data hendaklah mematuhi keperluan yang terpakai di bawah Akta 709 berhubung dengan pemprosesan data peribadi sensitif.

9.2 Persetujuan secara nyata hendaklah diperoleh sekiranya dikehendaki di bawah Akta 709 bagi pemprosesan data peribadi sensitif, termasuk apabila pemprosesan tersebut dijalankan melalui sistem AI, melainkan pemprosesan tersebut selainnya dibenarkan di bawah Akta 709.

9.3 Sekiranya persetujuan secara nyata dijadikan asas pemprosesan, pengawal data hendaklah memaklumkan dengan jelas kepada subjek data mengenai kategori data peribadi sensitif yang diproses, tujuan pemprosesan dan jika berkenaan, penggunaan sistem AI yang dimaksudkan.

9.4 Sebelum memproses data peribadi sensitif melalui sistem AI, pengawal data hendaklah menilai sama ada pemprosesan tersebut perlu dan berkadar, dengan mengambil kira sifat dan tahap sensitiviti data peribadi serta maksud pemprosesan tersebut.

10. Pemprosesan Tanpa Persetujuan dan Pengecualian

10.1 Sekiranya data peribadi diproses tanpa persetujuan, termasuk melalui sistem AI, pengawal data hendaklah memastikan bahawa pemprosesan tersebut dibenarkan di bawah Akta 709.

10.2 Bergantung pada peruntukan Akta 709 yang terpakai, data peribadi boleh diproses, termasuk melalui sistem AI, tanpa persetujuan sekiranya pemprosesan tersebut diperlukan bagi maksud yang dibenarkan di bawah Akta 709, termasuk bagi pelaksanaan kontrak, pematuhan kepada kewajipan undang-undang, perlindungan kepentingan vital subjek data, pentadbiran keadilan atau pelaksanaan fungsi yang diberikan oleh atau di bawah mana-mana undang-undang bertulis.

10.3 Sekiranya sesuatu pengecualian di bawah Akta 709 dijadikan sandaran berhubung dengan pemprosesan data peribadi, termasuk pemprosesan melalui sistem AI, pengawal data hendaklah menentukan pengecualian yang terpakai, memastikan bahawa syarat yang berkaitan dipenuhi, dan menggunakan pengecualian tersebut hanya setakat yang dibenarkan di bawah Akta 709. Pengawal data hendaklah terus mematuhi mana-mana keperluan di bawah Akta 709 yang tidak tertakluk kepada pengecualian tersebut.

10.4 Bergantung pada peruntukan Akta 709 yang terpakai, pengecualian daripada keperluan tertentu boleh terpakai kepada pemprosesan yang dijalankan melalui sistem AI bagi maksud atau dalam keadaan tertentu, termasuk pemprosesan yang berkaitan dengan pencegahan atau pengesanan jenayah, penyiasatan, penangkapan atau pendakwaan pesalah, pentaksiran atau pemungutan cukai atau duti, kesihatan fizikal atau mental, penyelidikan atau statistik, kewartawanan, kesusasteraan atau kesenian. Apa-apa pengecualian tersebut hendaklah terpakai hanya setakat dan tertakluk kepada syarat yang diperuntukkan di bawah Akta 709.

BAHAGIAN D: PEMBANGUNAN DAN PENGUJIAN SISTEM AI

11. Keperluan Am bagi Pembangunan Sistem AI

11.1 Pengawal data yang mereka bentuk, membangunkan, menguji atau mengesahkan sistem AI yang memproses data peribadi hendaklah melaksanakan langkah perlindungan teknikal dan organisasi yang bersesuaian sepanjang peringkat tersebut bagi memastikan pematuhan terhadap Akta 709.

11.2 Perlindungan data peribadi hendaklah diambil kira dari peringkat reka bentuk dan sepanjang pembangunan, latihan, pengujian dan pengesahan sistem AI, dengan mengambil kira sifat, skop, konteks dan maksud pemprosesan serta potensi risiko kepada subjek data.

11.3 Dalam melaksanakan perenggan 11.2, pengawal data hendaklah menerapkan konsep Mereka Bentuk Berdasarkan Perlindungan Data (Data Protection by Design – DPbD) dalam reka bentuk dan pembangunan sistem AI serta mengambil kira Garis Panduan Mereka Bentuk Berdasarkan Perlindungan Data yang dikeluarkan oleh Pesuruhjaya.

11.4 Sekiranya perubahan ketara dibuat terhadap sesuatu sistem AI semasa pembangunan atau pengujian yang boleh memberikan kesan material terhadap pemprosesan data peribadi, pengawal data hendaklah menentukan sama ada penilaian, pengujian atau pengesahan tambahan diperlukan sebelum meneruskan ke peringkat pembangunan atau pelaksanaan yang seterusnya.

12. Pengumpulan dan Penyediaan Data bagi Pembangunan AI

12.1 Data peribadi yang digunakan bagi pembangunan, pengujian, pengesahan atau penambahbaikan sistem AI hendaklah dikumpul dan diproses selaras dengan Akta 709.

12.2 Pengawal data hendaklah memastikan bahawa data peribadi yang digunakan untuk pembangunan, latihan, pengujian atau pengesahan sistem AI adalah mencukupi, relevan dan terhad kepada apa yang perlu bagi tujuan yang dimaksudkan.

12.3 Sekiranya data peribadi diperoleh daripada pelbagai sumber atau sumber luaran, pengawal data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi tersebut adalah tepat, lengkap dan, jika perlu, sentiasa dikemas kini sebelum digunakan bagi pembangunan, latihan, pengujian atau pengesahan.

12.4 Sekiranya tujuan pembangunan, latihan, pengujian atau pengesahan tersebut boleh dicapai secara munasabah tanpa mengenal pasti subjek data secara langsung, pengawal data hendaklah mempertimbangkan penggunaan data yang

dinyahnamakan *(anonymised)* atau disamarkan (*pseudonymised*), dengan mengambil kira langkah perlindungan yang dinyatakan dalam **Bahagian H** Kerangka ini.

13. Pembangunan Sistem AI

13.1 Sistem AI yang memproses data peribadi hendaklah dibangunkan menggunakan set data yang wajar, relevan dan sesuai bagi maksud penggunaan sistem tersebut.

13.2 Semasa pembangunan, pengawal data hendaklah mengambil langkah yang munasabah untuk mengenal pasti dan menangani isu yang boleh dijangka berpunca daripada data peribadi, set data atau reka bentuk sistem AI yang boleh menjejaskan secara material pemprosesan data peribadi atau subjek data.

13.3 Langkah teknikal dan organisasi yang bersesuaian hendaklah dilaksanakan sepanjang proses pembangunan untuk melindungi data peribadi daripada pemprosesan tanpa kebenaran atau menyalahi undang-undang, kehilangan secara tidak sengaja, salah guna, pengubahan atau penzahiran.

14. Pengujian dan Pengesahan Sebelum Pelaksanaan

14.1 Sebelum pelaksanaan, pengawal data hendaklah memastikan bahawa sistem AI yang memproses data peribadi diuji dan disahkan sewajarnya untuk mengesahkan bahawa sistem tersebut berfungsi selaras dengan maksud penggunaannya dan memproses data peribadi selaras dengan Akta 709.

14.2 Mengikut kesesuaian, pengujian dan pengesahan hendaklah menilai sama ada sistem AI:

(a) berfungsi selaras dengan maksud penggunaannya;

(b) menghasilkan output yang cukup boleh dipercayai bagi penggunaan yang dimaksudkan;

(c) beroperasi sebagaimana yang dimaksudkan dalam keadaan operasi yang boleh dijangka secara munasabah;

(d) menunjukkan ralat ketara, keterbatasan atau tingkah laku yang tidak dijangka yang boleh menjejaskan pemprosesan data peribadi atau subjek data; dan

(e) beroperasi secara berkesan dengan langkah perlindungan dan kawalan yang ditetapkan bagi pelaksanaan.

14.3 Sekiranya pengujian atau pengesahan melibatkan penggunaan data peribadi, pengawal data hendaklah memastikan bahawa hanya data peribadi yang bersesuaian dan diperlukan bagi maksud pengujian atau pengesahan tersebut digunakan, dan langkah perlindungan yang bersesuaian dilaksanakan untuk melindungi data peribadi tersebut.

14.4 Sekiranya pengujian atau pengesahan mengenal pasti isu ketara yang boleh menjejaskan pemprosesan data peribadi atau pematuhan terhadap Akta 709, pengawal data hendaklah memastikan bahawa langkah pembetulan yang bersesuaian diambil sebelum sistem AI tersebut dilaksanakan.

14.5 Sistem AI hendaklah diteruskan ke peringkat pelaksanaan hanya selepas pengawal data berpuas hati secara munasabah bahawa pengujian dan pengesahan yang berkaitan telah diselesaikan dan apa-apa isu ketara yang dikenal pasti telah ditangani dengan sewajarnya.

BAHAGIAN E: PELAKSANAAN DAN PENGGUNAAN SISTEM AI DALAM PEMPROSESAN DATA PERIBADI

15. Pelaksanaan Sistem AI

15.1 Sebelum melaksanakan sistem AI yang memproses data peribadi, pengawal data hendaklah memastikan bahawa sistem AI tersebut telah melalui pengujian dan pengesahan yang berkaitan di bawah **Bahagian D** dan sesuai bagi maksud penggunaannya.

15.2 Pengawal data hendaklah memastikan bahawa sistem AI dilaksanakan dan dikonfigurasikan dengan cara yang selaras dengan maksud penggunaannya, asas undang-undang terpakai sebagaimana yang ditetapkan di bawah **Bahagian C** Kerangka ini dan keperluan di bawah Akta 709.

15.3 Sekiranya sistem AI diintegrasikan dengan sistem maklumat, pangkalan data, aplikasi atau perkhidmatan luaran sedia ada, pengawal data hendaklah mengambil langkah yang bersesuaian untuk memastikan bahawa pengintegrasian tersebut tidak mengakibatkan pemprosesan data peribadi dengan cara yang tidak selaras dengan maksud pemprosesan atau Akta 709.

15.4 Pengawal data hendaklah memastikan bahawa pelaksanaan dan penggunaan sistem AI diberi kebenaran sewajarnya selaras dengan dasar dan aturan tadbir urus organisasi yang terpakai.

16. Penggunaan Sistem AI dalam Pemprosesan Data Peribadi

16.1 Semasa pengoperasian sesuatu sistem AI, pengawal data hendaklah memastikan bahawa data peribadi diproses selaras dengan asas perundangan yang terpakai di bawah Akta 709 dan konsisten dengan maksud yang baginya data peribadi tersebut boleh diproses.

16.2 Pengawal data hendaklah memastikan bahawa data peribadi yang dimasukkan ke dalam, diakses oleh, dijana melalui atau selainnya diproses menggunakan sistem AI adalah mencukupi, relevan dan tidak berlebihan berhubung dengan maksud pemprosesan tersebut.

16.3 Pengawal data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa kakitangan yang diberi kuasa untuk menggunakan sistem AI memproses data peribadi hanya bagi tujuan yang dibenarkan dan selaras dengan dasar dan prosedur organisasi yang terpakai.

16.4 Data peribadi tidak boleh dimasukkan ke dalam atau diproses melalui sistem AI sekiranya penggunaan sistem AI tersebut bagi pemprosesan berkenaan tidak dibenarkan oleh pengawal data.

Contoh:

Sebuah platform e-dagang menggunakan sistem AI untuk mencadangkan produk kepada pengguna berdasarkan sejarah pembelian dan pelayaran mereka. Pengawal data memastikan bahawa sistem AI hanya menggunakan data peribadi yang relevan dan tidak berlebihan bagi maksud menghasilkan syor tersebut. Data peribadi yang dikumpul bagi maksud yang tidak berkaitan tidak digunakan oleh sistem AI untuk menghasilkan syor berkenaan.

17. Pemantauan Operasi

17.1 Pengawal data hendaklah mewujudkan proses yang bersesuaian untuk memantau sistem AI sepanjang kitaran hayat operasinya bagi menilai sama ada perubahan dalam pengoperasian, data peribadi yang diproses atau persekitaran operasi boleh menjejaskan pematuhan terhadap Akta 709 atau meningkatkan risiko kepada subjek data.

17.2 Pengawal data hendaklah menyemak secara berkala sama ada data peribadi yang diproses oleh sistem AI kekal mencukupi, relevan dan tidak berlebihan berhubung dengan maksud pemprosesan tersebut.

17.3 Sekiranya pemantauan mengenal pasti isu ketara yang boleh menjejaskan pemprosesan data peribadi atau subjek data, pengawal data hendaklah mengambil langkah pembetulan yang bersesuaian, yang boleh termasuk mengemas kini sistem AI, melaksanakan langkah perlindungan tambahan atau mengehadkan pemprosesan yang berkaitan sehingga isu tersebut ditangani dengan sewajarnya.

17.4 Penemuan pemantauan yang signifikan dan langkah pembetulan yang diambil hendaklah didokumenkan selaras dengan **Bahagian J** Kerangka ini mengikut kesesuaian.

Contoh:

Sebuah platform e-dagang menggunakan sistem AI untuk mencadangkan produk berdasarkan sejarah pelayaran dan pembelian pengguna. Semasa pemantauan operasi, platform tersebut mendapati bahawa selepas pengemaskinian sistem, sistem AI menggunakan data peribadi yang tidak dimaksudkan untuk digunakan bagi menghasilkan syor produk. Platform tersebut mengehadkan pemprosesan yang terjejas sehingga isu berkenaan disiasat dan diperbetulkan.

18. Pengubahsuaian, Latihan Semula dan Penggunaan Berterusan

18.1 Sekiranya sesuatu sistem AI diubah suai, dilatih semula atau dikemas kini selepas pelaksanaan, pengawal data hendaklah menentukan sama ada perubahan tersebut memberikan kesan material terhadap pemprosesan data peribadi atau maksud penggunaan sistem AI tersebut.

18.2 Sekiranya sesuatu perubahan boleh memberikan kesan material, pengawal data hendaklah memastikan bahawa penilaian, pengujian atau pengesahan yang bersesuaian dilaksanakan selaras dengan **Bahagian D** sebelum sistem AI yang diubah suai atau dilatih semula tersebut digunakan.

18.3 Pengawal data hendaklah menyemak secara berkala sama ada sistem AI yang telah dilaksanakan kekal sesuai bagi maksud penggunaannya dan sama ada penggunaan berterusan sistem AI tersebut kekal selaras dengan Akta 709.

Contoh:

Sebuah organisasi menggunakan chatbot AI untuk menjawab pertanyaan pelanggan. *Chatbot* tersebut kemudiannya dilatih semula menggunakan data pelanggan tambahan dan fungsi baharu diperkenalkan. Sebelum menggunakan *chatbot* yang telah dikemas kini, pengawal data menilai sama ada perubahan tersebut memberikan kesan material terhadap pemprosesan data peribadi dan, jika perlu, menjalankan pengujian dan pengesahan lanjut selaras dengan **Bahagian D**.

19. Penamatan dan Pelucutan Operasi Sistem AI

19.1 Sekiranya sistem AI yang memproses data peribadi ditamatkan atau dilucutkan operasi, pengawal data hendaklah memastikan bahawa semua data peribadi yang berkaitan dengan sistem AI tersebut terus dikendalikan selaras dengan Akta 709.

19.2 Sebelum pelucutan operasi, pengawal data hendaklah menentukan langkah yang bersesuaian bagi penyimpanan, pemindahan, penyahnamaan atau pelupusan data peribadi secara selamat, dengan mengambil kira maksud asal pemprosesan, Prinsip Penyimpanan di bawah Akta 709 dan apa-apa keperluan yang terpakai di bawah mana-mana undang-undang bertulis yang lain.

19.3 Data peribadi tidak boleh disimpan semata-mata kerana data tersebut telah digunakan oleh atau dikaitkan dengan sistem AI yang telah dilucutkan operasi. Sekiranya data peribadi tersebut tidak lagi diperlukan, data tersebut hendaklah dipadamkan dengan selamat, dinyahnamakan atau dilupuskan selaras dengan Akta 709 dan mana-mana undang-undang bertulis yang terpakai.

BAHAGIAN F: PEROLEHAN, INTEGRASI DAN PENGURUSAN SISTEM AI LUARAN

20. Pengurusan Sistem AI Luaran dan Penyedia Perkhidmatan

20.1 Pengawal data boleh melantik penyedia perkhidmatan AI termasuk pembangun, vendor atau penyedia perkhidmatan awan untuk mereka bentuk, membangunkan, menyesuaikan, melaksanakan, menghos, mengendalikan, menyelenggara atau menyokong sistem AI yang memproses data peribadi.

20.2 Sebelum memperoleh, mengintegrasikan atau menggunakan sistem AI luaran, pengawal data hendaklah menjalankan usaha wajar *(due diligence)* yang bersesuaian dengan mengambil kira:

(a) maksud penggunaan, fungsi dan batasan sistem AI;

(b) kategori dan sensitiviti data peribadi yang akan diproses;

(c) sumber dan kualiti set data atau model pra-latihan yang berkaitan, sekiranya maklumat tersebut boleh diperoleh secara munasabah;

(d) sama ada data peribadi akan disimpan, digunakan semula atau digunakan bagi latihan model, penentukuran halus (fine-tuning), pengoptimuman, analitik atau maksud lain di luar perkhidmatan yang dimaksudkan;

(e) penglibatan pemproses data lain atau penyedia perkhidmatan pihak ketiga;

(f) apa-apa pemprosesan atau pemindahan data peribadi rentas sempadan, jika berkenaan;

(g) langkah teknikal dan organisasi yang dilaksanakan oleh penyedia bagi melindungi data peribadi; dan

(h) apa-apa risiko, kecenderungan berat sebelah (bias) atau batasan yang diketahui yang boleh menjejaskan pemprosesan data peribadi atau subjek data.

20.3 Tahap usaha wajar hendaklah berkadar dengan sifat dan sensitiviti data peribadi, maksud penggunaan sistem AI dan potensi risiko terhadap subjek data.

21. Peranan, Tanggungjawab dan Sempadan Pemprosesan Data

21.1 Sekiranya penyedia perkhidmatan AI terlibat dalam pemprosesan data peribadi, pengawal data hendaklah menentukan dan memperincikan dengan jelas peranan dan tanggungjawab pihak yang berkaitan di bawah Akta 709, dengan mengambil kira penglibatan sebenar mereka dalam pemprosesan tersebut.

21.2 Ini hendaklah termasuk menentukan sama ada penyedia perkhidmatan AI bertindak sebagai pemproses data yang memproses data peribadi bagi pihak dan mengikut arahan pengawal data, atau selainnya bertindak sebagai pihak ketiga di bawah Akta 709.

21.3 Sekiranya penyedia perkhidmatan AI memproses data peribadi bagi pihak pengawal data, pengaturan yang bersesuaian hendaklah diwujudkan bagi mengawal pemprosesan data peribadi, termasuk jika berkenaan:

(a) sifat dan maksud pemprosesan;

(b) kategori data peribadi yang terlibat;

(c) arahan pengawal data;

(d) langkah yang bersesuaian untuk melindungi data peribadi;

(e) penglibatan pemproses data lain atau penyedia perkhidmatan pihak ketiga;

(f) pengendalian insiden keselamatan atau pelanggaran data peribadi; dan

(g) pemulangan, pemadaman atau pelupusan data peribadi secara selamat apabila perkhidmatan ditamatkan atau apabila data peribadi tidak lagi diperlukan, tertakluk kepada Akta 709 atau mana-mana undang-undang bertulis lain terpakai.

21.4 Pengawal data boleh meminta dokumentasi atau maklumat yang bersesuaian daripada penyedia perkhidmatan AI seperti kad model (*model cards*), kad sistem (*system cards*) atau dokumentasi teknikal apabila semunasabahnya diperlukan untuk memahami fungsi, pengoperasian, amalan pemprosesan data peribadi dan batasan sistem AI luaran.

Contoh:

Pengawal data boleh mendapatkan maklumat daripada penyedia perkhidmatan AI mengenai cara data peribadi diproses dan menetapkan pengaturan yang

bersesuaian untuk mengehadkan penyimpanan, penggunaan semula atau penggunaan sekunder data peribadi di luar maksud pemprosesan yang ditetapkan.

21.5 Pelantikan penyedia perkhidmatan AI tidak memindahkan atau mengurangkan tanggungjawab pengawal data di bawah Akta 709.

22. Pemprosesan dan Pemindahan Data Peribadi Rentas Sempadan

22.1 Sekiranya perolehan, integrasi atau penggunaan sistem AI luaran melibatkan pemindahan data peribadi ke luar Malaysia, pengawal data hendaklah memastikan pemindahan tersebut mematuhi seksyen 129 Akta 709.

22.2 Sekiranya bersesuaian, pengawal data hendaklah menjalankan Penilaian Impak Pemindahan (Transfer Impact Assessment - "TIA"), dengan merujuk kepada Garis Panduan Pemindahan Data Peribadi Rentas Sempadan yang terpakai yang dikeluarkan oleh Pesuruhjaya, bagi menilai tahap perlindungan data peribadi yang diberikan di tempat data peribadi tersebut dipindahkan dan langkah perlindungan yang terpakai terhadap pemindahan tersebut.

22.3 Dalam menilai pemindahan rentas sempadan yang melibatkan sistem AI luaran, pengawal data hendaklah, sekiranya bersesuaian, mengambil kira:

(a) negara di mana data peribadi akan disimpan atau diproses;

(b) pihak yang mungkin mempunyai akses kepada data peribadi;

(c) amalan pengendalian dan perlindungan data peribadi oleh penyedia perkhidmatan AI dan pihak lain yang terlibat, khususnya apabila data peribadi diproses merentasi pelbagai bidang kuasa;

(d) langkah perlindungan yang terpakai terhadap pemindahan dan pemprosesan selanjutnya; dan

(e) apa-apa pemindahan seterusnya atau penzahiran data peribadi oleh penyedia perkhidmatan AI kepada pemproses data lain atau penyedia perkhidmatan pihak ketiga.

22.4 Pengawal data hendaklah menyenggara rekod yang bersesuaian mengenai pemindahan rentas sempadan dan langkah perlindungan yang dilaksanakan bagi menyokong pematuhan terhadap seksyen 129 Akta 709.

23. Pengawasan Berterusan Sistem AI Luaran

23.1 Pengawal data hendaklah mengekalkan pengawasan yang bersesuaian terhadap sistem AI luaran dan penyedia perkhidmatan sepanjang tempoh data peribadi diproses melalui sistem atau perkhidmatan tersebut.

23.2 Di mana terdapat perubahan ketara terhadap sistem AI luaran, terma perkhidmatan, aktiviti pemprosesan, penglibatan pemproses data lain atau penyedia perkhidmatan pihak ketiga, atau amalan pengendalian data, pengawal data hendaklah menilai sama ada langkah perlindungan tambahan, perubahan kepada pengaturan sedia ada atau semakan lanjut diperlukan sebelum meneruskan penggunaan sistem AI tersebut.

BAHAGIAN G: HAK SUBJEK DATA DALAM SISTEM AI

24. Hak Subjek Data dalam Sistem AI

24.1 Hak subjek data di bawah Akta 709 terus terpakai sekiranya data peribadi diproses melalui sistem AI.

24.2 Pengawal data hendaklah melaksanakan proses yang bersesuaian bagi memudahkan pelaksanaan hak tersebut selaras dengan Akta 709 dengan mengambil kira cara data peribadi diproses oleh sistem AI.

25. Hak untuk Mengakses Data Peribadi

25.1 Pengawal data hendaklah memastikan bahawa atas permintaan, subjek data diberikan akses kepada data peribadinya yang diproses melalui sistem AI tertakluk kepada Akta 709 dan mana-mana pengecualian atau sekatan yang terpakai.

25.2 Sekiranya terpakai, data peribadi yang boleh diakses di bawah perenggan 25.1 boleh merangkumi data peribadi yang dijana atau diterbitkan melalui sistem AI yang berkaitan dengan subjek data, di mana data peribadi tersebut boleh dikenal pasti dan diperoleh semula secara munasabah.

26. Hak untuk Membetulkan Data Peribadi

26.1 Subjek data boleh meminta pembetulan data peribadinya yang diproses melalui sistem AI sekiranya data peribadi tersebut tidak tepat, tidak lengkap, mengelirukan atau tidak terkini selaras dengan Akta 709.

26.2 Sekiranya sistem AI menyebabkan atau menyumbang kepada ketidaktepatan data peribadi, pengawal data hendaklah mengambil langkah yang bersesuaian untuk mengesahkan dan membetulkan data peribadi tersebut dan sekiranya bersesuaian, menangani punca ketidaktepatan tersebut.

27. Hak untuk Menarik Balik Persetujuan

27.1 Subjek data boleh menarik balik persetujuannya terhadap pemprosesan data peribadinya selaras dengan Akta 709. Sekiranya data peribadi tersebut diproses melalui sistem AI, penarikan balik persetujuan tersebut hendaklah turut terpakai kepada pemprosesan data peribadi melalui sistem AI bagi maksud yang berkaitan.

27.2 Apabila persetujuan ditarik balik, pengawal data hendaklah menghentikan pemprosesan data peribadi bagi maksud yang berkaitan, termasuk pemprosesannya melalui sistem AI, tertakluk kepada Akta 709 dan apa-apa pengecualian atau sekatan yang terpakai.

28. Hak kepada Kemudahalihan Data

28.1 Sekiranya hak kepada kemudahalihan data di bawah Akta 709 terpakai, pengawal data hendaklah memudahkan penghantaran data peribadi subjek data selaras dengan keperluan yang terpakai di bawah Akta 709.

28.2 Sekiranya data peribadi yang diproses melalui sistem AI tertakluk kepada permintaan kemudahalihan data, pengawal data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa penghantaran tersebut tidak menjejaskan keselamatan, kerahsiaan atau integriti data peribadi tersebut.

29. Memudahkan Pelaksanaan Hak Subjek Data

29.1 Di mana sistem AI, termasuk model AI tujuan umum atau sistem AI yang terbenam di dalam aplikasi, antara muka atau aliran kerja, memproses data peribadi menerusi cara yang mungkin tidak nyata kepada subjek data, pengawal data hendaklah, mengikut kesesuaian, melaksanakan langkah-langkah ketelusan tambahan bagi memudahkan pelaksanaan hak-hak subjek data secara berkesan di bawah Akta 709.

29.2 Pengawal data hendaklah menyediakan mekanisme yang jelas dan mudah diakses bagi membolehkan subjek data melaksanakan haknya di bawah Akta 709 yang boleh merangkumi, jika bersesuaian, tetapan akaun, borang dalam talian, komunikasi elektronik atau saluran lain yang bersesuaian.

29.3 Bagi menyokong pelaksanaan hak subjek data secara berkesan di bawah Akta 709, pengawal data hendaklah, sekiranya bersesuaian:

(a) menyediakan maklumat yang jelas dan mudah diakses mengenai cara subjek data boleh melaksanakan haknya berhubung dengan data peribadi yang diproses melalui sistem AI;

(b) menyediakan penjelasan yang bersesuaian bagi membantu subjek data memahami bagaimana pemprosesan data peribadi melalui sistem AI berkaitan dengan pelaksanaan haknya; dan

(c) menyediakan saluran yang mudah diakses bagi mengendalikan permintaan berkaitan pelaksanaan hak subjek data di bawah Akta 709.

BAHAGIAN H: LANGKAH PERLINDUNGAN UTAMA DAN OBLIGASI KESAKSAMAAN DALAM SISTEM AI

30. Langkah Perlindungan Utama dan Obligasi Kesaksamaan dalam Sistem AI

30.1 Bagi menyokong penggunaan sistem AI yang memproses data peribadi secara bertanggungjawab, pengawal data hendaklah melaksanakan langkah perlindungan dan langkah kesaksamaan yang bersesuaian sepanjang kitaran hayat sistem AI.

30.2 Langkah yang dilaksanakan di bawah Bahagian ini hendaklah berkadar dengan sifat, skop, konteks dan maksud pemprosesan, kategori data peribadi yang terlibat serta potensi risiko terhadap subjek data.

Nota:

Pengawal data boleh mempertimbangkan garis panduan etika atau tadbir urus AI yang relevan, termasuk yang dikeluarkan di peringkat kebangsaan, mengikut kesesuaian.

31. Kesaksamaan dan Pencegahan Hasil yang Tidak Adil

31.1 Sistem AI yang memproses data peribadi hendaklah direka bentuk, diuji, digunakan dan dipantau dengan cara yang meminimumkan risiko yang boleh dijangka terhadap hasil yang tidak adil, berat sebelah atau bersifat diskriminasi yang menjejaskan subjek data, termasuk risiko yang timbul daripada ciri-ciri seperti bangsa, jantina, agama, umur, ketidakupayaan atau ciri lain yang berkaitan.

31.2 Dalam menangani risiko tersebut, pengawal data hendaklah, mengikut kesesuaian:

(a) menilai data latihan, pengujian dan pengoperasian dari segi kualiti, keterwakilan dan potensi kecenderungan berat sebelah;

(b) menyemak output yang dijana AI bagi mengenal pasti kecenderungan berat sebelah, ketidakadilan atau corak diskriminasi yang material;

(c) melaksanakan langkah pembetulan yang bersesuaian sekiranya isu material dikenal pasti; dan

(d) mewujudkan mekanisme semakan atau eskalasi yang bersesuaian sekiranya output yang dijana AI boleh memberi kesan ketara kepada subjek data.

32. Langkah Perlindungan Keselamatan

32.1 Pengawal data hendaklah melaksanakan langkah teknikal dan organisasi yang bersesuaian untuk melindungi data peribadi yang diproses melalui sistem AI selaras dengan Prinsip Keselamatan di bawah Akta 709.

32.2 Langkah keselamatan yang dilaksanakan hendaklah berkadar dengan sifat dan tahap sensitiviti data peribadi yang diproses, sifat pemprosesan, keupayaan keselamatan sistem AI dan potensi risiko kepada subjek data.

32.3 Data peribadi hendaklah dilindungi sepanjang pemprosesannya melalui sistem AI, termasuk semasa pengumpulan, penghantaran, penyimpanan, penggunaan, akses dan pelupusan.

32.4 Langkah-langkah keselamatan yang bersesuaian boleh termasuk, mengikut kesesuaian:

(a) kawalan akses dan mekanisme pengesahan;

(b) penyulitan dan penghantaran data peribadi secara selamat;

(c) konfigurasi selamat, penampalan (patching) dan pengemaskinian komponen sistem yang berkaitan;

(d) pengelogan dan pemantauan akses kepada data peribadi;

(e) pengasingan atau perlindungan tambahan terhadap data peribadi sensitif; dan

(f) prosedur tindak balas insiden.

32.5 Langkah-langkah tambahan boleh dipertimbangkan sekiranya bersesuaian bagi menangani risiko yang timbul daripada ciri-ciri khusus sistem AI seperti:

(a) melaksanakan kawalan Pencegahan Kehilangan Data (Data Loss Prevention – DLP) untuk mengesan dan menghalang penghantaran atau penyerahan data peribadi tanpa kebenaran, termasuk pengecam kepada model AI luaran atau API;

(b) menggunakan protokol komunikasi yang selamat dan disulitkan untuk perkhidmatan AI luaran, termasuk LLM;

(c) menguatkuasakan kawalan akses yang bersesuaian terhadap sistem AI atas dasar "perlu tahu" *(need-to-know basis)*;

(d) mengasingkan atau menyulitkan data peribadi sensitif semasa latihan, pengujian, pelaksanaan atau inferens, sekiranya bersesuaian; dan

(e) menilai konfigurasi keselamatan sistem AI terbenam *(embedded AI systems),* termasuk di peringkat peranti dan sistem, bagi memastikan data peribadi dilindungi dengan sewajarnya.

33. Insiden Keselamatan dan Pelanggaran Data Peribadi

33.1 Pengawal data hendaklah mewujudkan prosedur yang bersesuaian untuk mengenal pasti, menilai, mengurus dan bertindak balas terhadap insiden keselamatan yang melibatkan data peribadi yang diproses melalui sistem AI.

33.2 Sekiranya pengawal data mempunyai sebab untuk mempercayai bahawa suatu pelanggaran data peribadi telah berlaku berhubung dengan sistem AI, pengawal data hendaklah menilai pelanggaran tersebut dan mematuhi kewajipan pemberitahuan yang terpakai di bawah seksyen 12B Akta 709.

33.3 Sekiranya pemberitahuan dikehendaki di bawah seksyen 12B Akta 709, pengawal data hendaklah mematuhi keperluan, tempoh masa dan tatacara yang terpakai di bawah Akta 709 serta Pekeliling dan Garis Panduan mengenai Pemberitahuan Pelanggaran Data yang dikeluarkan oleh Pesuruhjaya.

33.4 Pengawal data hendaklah mengambil langkah yang bersesuaian untuk membendung dan mengurangkan kesan pelanggaran data peribadi yang melibatkan sistem AI dan, jika perlu, menangani puncanya bagi mengurangkan kemungkinan kejadian tersebut berulang.

33.5 Sekiranya pelanggaran data peribadi melibatkan pemproses data atau penyedia perkhidmatan AI, pengawal data hendaklah memastikan bahawa pengaturan yang bersesuaian diwujudkan bagi membolehkan penyampaian maklumat yang diperlukan secara tepat pada masanya untuk pengawal data mematuhi seksyen 12B Akta 709.

34. Ketepatan dan Integriti Data

34.1 Selaras dengan Prinsip Integriti Data di bawah Akta 709, pengawal data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi yang diproses melalui sistem AI adalah tepat, lengkap, tidak mengelirukan dan dikemas kini setakat yang perlu, dengan mengambil kira maksud yang baginya data peribadi tersebut diproses.

34.2 Pengawal data hendaklah mewujudkan proses yang bersesuaian untuk mengenal pasti, menyemak dan membetulkan ketidaktepatan dalam data peribadi yang digunakan sebagai input atau terkandung dalam output yang dijana oleh AI serta mencegah ketidaktepatan tersebut daripada dijadikan sandaran bagi pemprosesan selanjutnya atau keputusan yang boleh memberi kesan ketara kepada subjek data.

BAHAGIAN I: TADBIR URUS DAN PENGURUSAN RISIKO

35. Tadbir Urus dan Pengawasan Organisasi

35.1 Pengawal data hendaklah mewujudkan aturan tadbir urus yang bersesuaian bagi sistem AI yang memproses data peribadi untuk menyokong pengawasan yang berkesan, akauntabiliti dan pematuhan terhadap Akta 709 sepanjang kitaran hayat sistem AI.

35.2 Aturan tadbir urus tersebut hendaklah berkadar dengan sifat, skop, konteks dan maksud pemprosesan, dengan mengambil kira kategori data peribadi yang diproses, kerumitan sistem AI dan potensi risiko terhadap subjek data.

35.3 Pengawal data hendaklah menetapkan dengan jelas peranan dan tanggungjawab bagi tadbir urus, pengoperasian, pemantauan dan pengawasan sistem AI kepada kakitangan atau fungsi yang bersesuaian dalam organisasi.

35.4 Sekiranya Pegawai Perlindungan Data dilantik atau dikehendaki di bawah Akta 709, Pegawai Perlindungan Data hendaklah dilibatkan dengan sewajarnya dalam pengawasan pemprosesan data peribadi melalui sistem AI, dengan mengambil kira sifat dan risiko pemprosesan tersebut.

35.5 Keputusan signifikan atau isu material berkaitan sistem AI yang boleh memberikan kesan material terhadap pemprosesan data peribadi atau subjek data hendaklah tertakluk kepada semakan, rujukan kepada peringkat pengurusan yang bersesuaian atau kelulusan dalam organisasi.

36. Polisi, Prosedur dan Kesedaran

36.1 Pengawal data hendaklah mewujudkan dasar dan prosedur dalaman yang bersesuaian bagi mengawal selia pembangunan, pelaksanaan dan penggunaan sistem AI yang memproses data peribadi.

36.2 Kakitangan yang terlibat dalam pembangunan, pelaksanaan, pengoperasian, penggunaan atau pengawasan sistem AI hendaklah mempunyai pengetahuan yang bersesuaian mengenai tanggungjawab mereka di bawah Akta 709 serta menerima latihan dan kesedaran yang bersesuaian dengan peranan masing-masing.

36.3 Dasar dan prosedur tersebut hendaklah, mengikut kesesuaian, merangkumi tanggungjawab yang terpakai, proses kelulusan, sekatan penggunaan dan kawalan berkaitan pemprosesan data peribadi melalui sistem AI.

36.4 Pengawal data hendaklah, mengikut kesesuaian, mengkonfigurasikan sistem AI supaya menggunakan tetapan pemeliharaan privasi secara lalai *(privacy-preserving settings by default)* dengan mengambil kira sifat dan maksud pemprosesan serta risiko terhadap subjek data.

36.5 Dasar dan prosedur dalaman hendaklah disemak secara berkala dan dikemas kini apabila perlu bagi mencerminkan perubahan material kepada sistem AI, keperluan perundangan yang terpakai atau amalan organisasi.

37. Pengurusan Risiko

37.1 Pengawal data hendaklah mengguna pakai pendekatan berasaskan risiko terhadap

pemprosesan data peribadi melalui sistem AI dan menjalankan penilaian risiko serta impak yang bersesuaian bagi mengenal pasti, menilai dan mengurangkan risiko privasi dan perlindungan data peribadi yang berpotensi, dengan mengambil kira sifat, skop, konteks dan maksud pemprosesan serta potensi risiko terhadap subjek data.

37.2 Dalam menilai risiko yang berkaitan dengan sistem AI, pengawal data hendaklah, sekiranya bersesuaian, mengambil kira:

(a) jenis, jumlah, sifat dan sensitiviti data peribadi yang diproses;

(b) maksud dan penggunaan sistem AI;

(c) kerumitan dan fungsi sistem AI;

(d) potensi output yang tidak tepat, berat sebelah, tidak adil atau mengelirukan yang boleh menjejaskan subjek data;

(e) risiko penyalahgunaan, pemprosesan berlebihan, akses atau penzahiran tanpa kebenaran, kehilangan, pengubahan, inferens atau pengenalpastian semula data peribadi;

(f) sejauh mana sistem AI membuat atau menyokong keputusan yang boleh memberi kesan signifikan kepada subjek data;

(g) kecukupan langkah perlindungan teknikal dan organisasi; dan

(h) kebarangkalian dan tahap keterukan potensi kesan buruk terhadap subjek data.

37.3 Jika bersesuaian, penilaian risiko hendaklah merangkumi, atau dilengkapi dengan, Penilaian Impak Perlindungan Data (DPIA), dengan mengambil kira apa-apa garis panduan terpakai yang dikeluarkan oleh Pesuruhjaya bagi mengenal pasti, menilai dan mengurangkan risiko yang timbul daripada pemprosesan data peribadi melalui sistem AI.

37.4 Sekiranya risiko yang ketara dikenal pasti, pengawal data hendaklah melaksanakan langkah teknikal, organisasi atau langkah lain yang bersesuaian untuk menghapuskan atau mengurangkan risiko tersebut sebelum melaksanakan atau meneruskan pengoperasian sistem AI. Langkah tersebut boleh termasuk:

(a) mengurangkan atau mengehadkan data peribadi yang diproses atau mengubah cara data peribadi diproses;

(b) melaksanakan langkah perlindungan teknikal dan organisasi yang bersesuaian, termasuk konfigurasi dan kawalan yang memelihara privasi;

(c) mengubah reka bentuk, konfigurasi, fungsi atau maksud penggunaan sistem AI, jika perlu;

(d) melaksanakan langkah pengujian, pemantauan, semakan atau pengawasan manusia yang bersesuaian; dan

(e) mengambil apa-apa langkah pembetulan atau mitigasi lain yang perlu untuk mengurangkan risiko yang dikenal pasti kepada tahap yang boleh diterima.

37.5 Penilaian risiko, termasuk mana-mana DPIA yang dijalankan, hendaklah disemak secara berkala dan sekiranya terdapat perubahan material kepada sistem AI, aktiviti pemprosesan, maksud penggunaan atau risiko yang dikenal pasti, termasuk kemas kini yang signifikan, latihan semula atau integrasi dengan sistem lain.

38. Ketelusan dan Kebolehjelasan

38.1 Pengawal data hendaklah memastikan bahawa subjek data dimaklumkan, melalui notis perlindungan data peribadi atau notis privasi yang jelas dan mudah diakses, mengenai pemprosesan data peribadinya melalui atau berhubung dengan sistem AI, dan mengenai haknya di bawah Akta 709. Ini termasuk, jika terpakai:

(a) maksud data peribadi tersebut diproses, termasuk keadaan di mana sistem AI digunakan bagi maksud tersebut;

(b) sama ada sistem AI digunakan untuk menghasilkan output, syor, ramalan atau keputusan lain yang melibatkan data peribadi subjek data yang boleh memberi kesan kepada subjek data tersebut; dan

(c) maklumat yang mencukupi dalam bahasa yang mudah difahami bagi membolehkan subjek data memahami maksud pemprosesan yang berkaitan dan bagaimana pemprosesan berkaitan AI tersebut boleh memberi kesan kepada subjek data.

39. Semakan Dalaman, Pembuktian Pematuhan dan Pengawasan Berterusan

39.1 Pengawal data hendaklah menyemak secara berkala aturan tadbir urusnya dan pengoperasian sistem AI yang memproses data peribadi bagi menyokong pematuhan berterusan terhadap Akta 709.

39.2 Semakan dalaman boleh termasuk audit, penilaian pematuhan, atau aktiviti jaminan yang lain mengikut kesesuaian dengan mengambil kira sifat dan risiko pemprosesan.

39.3 Pengawal data hendaklah menyenggara rekod yang bersesuaian bagi membuktikan pematuhan terhadap Akta 709 dan menyokong audit pada masa hadapan, termasuk, jika relevan, rekod mengenai keputusan reka bentuk, aliran data peribadi dan aktiviti pemprosesan lain, keputusan tadbir urus, penilaian risiko, DPIA, semakan material dan pengawasan terhadap penyedia perkhidmatan AI luaran. Rekod dan dokumentasi tersebut hendaklah, mengikut kesesuaian, mencerminkan dengan tepat pembangunan, pelaksanaan, pengoperasian dan pemprosesan data peribadi yang berkaitan melalui sistem AI.

39.4 Sekiranya kelemahan atau isu material dikenal pasti melalui pemantauan atau semakan, pengawal data hendaklah melaksanakan langkah pembetulan yang bersesuaian dalam tempoh yang munasabah, dengan mengambil kira sifat dan tahap keterukan isu yang dikenal pasti.

39.5 Sekiranya penyedia perkhidmatan AI atau sistem AI luaran terlibat, pengawal data hendaklah mengekalkan pengawasan yang bersesuaian selaras dengan **Bahagian F** Kerangka ini.

BAHAGIAN J: DOKUMENTASI, AUDIT DAN PEMATUHAN

40. Dokumentasi dan Penyimpanan Rekod

40.1 Pengawal data hendaklah menyelenggara dokumentasi dan rekod yang bersesuaian berkaitan sistem AI yang memproses data peribadi bagi menyokong akauntabiliti dan membuktikan pematuhan kepada Akta 709.

40.2 Dokumentasi dan rekod tersebut hendaklah, jika relevan, merangkumi pemprosesan data peribadi sepanjang kitaran hayat sistem AI.

40.3 Sifat dan tahap dokumentasi hendaklah berkadar dengan sifat, skop, konteks dan tujuan pemprosesan, dengan mengambil kira kerumitan sistem AI dan potensi risiko terhadap subjek data.

40.4 Jika bersesuaian, dokumentasi dan rekod hendaklah merangkumi:

(a) tujuan, kegunaan yang dimaksudkan, reka bentuk dan fungsi sistem AI;

(b) jenis dan sumber data peribadi yang diproses, termasuk sama ada data peribadi dikumpul secara langsung daripada subjek data atau diperoleh daripada sumber lain;

(c) asas undang-undang yang terpakai bagi pemprosesan data peribadi;

(d) penilaian, kelulusan dan keputusan material yang berkaitan dengan pemprosesan;

(e) perubahan ketara kepada sistem AI atau aktiviti pemprosesan;

(f) insiden, isu dan tindakan pembetulan yang material;

(g) penglibatan dan pengawasan berkaitan penyedia perkhidmatan AI, jika berkenaan; dan

(h) apa-apa rekod lain yang perlu bagi membuktikan pematuhan terhadap Akta 709.

40.5 Dokumen dan rekod hendaklah disemak dan dikemas kini jika perlu susulan perubahan material pada sistem AI atau aktiviti pemprosesannya dan hendaklah dikemukakan kepada Pesuruhjaya atas permintaan.

41. Semakan Dalaman dan Audit

41.1 Pengawal data hendaklah mewujudkan proses yang bersesuaian bagi semakan berkala dan jika berkenaan, audit ke atas sistem AI serta aktiviti pemprosesan yang berkaitan bagi menilai pematuhan berterusan terhadap Akta 709 serta dasar, prosedur dan tadbir urus organisasi yang terpakai.

41.2 Kekerapan dan skop semakan dalaman atau audit hendaklah berkadar dengan sifat, skop, konteks dan risiko pemprosesan data peribadi melalui sistem AI.

41.3 Semakan dalaman atau audit boleh, jika bersesuaian, menilai:

(a) pematuhan terhadap keperluan terpakai di bawah Akta 709 serta dasar, prosedur dan tadbir urus dalaman yang berkaitan;

(b) keberkesanan langkah-langkah teknikal dan organisasi yang dilaksanakan untuk melindungi data peribadi;

(c) pengurusan risiko yang dikenal pasti dan keberkesanan langkah perlindungan yang dilaksanakan;

(d) pematuhan terhadap pengaturan berkaitan yang melibatkan penyedia perkhidmatan AI;

(e) perubahan material, ralat, pergerakan model (*model drift*) atau isu lain yang boleh menjejaskan pemprosesan data peribadi;

(f) risiko baharu atau peningkatan risiko yang timbul daripada kemas kini, latihan semula (*retraining*), integrasi sistem, perubahan kepada aktiviti pemprosesan, atau perluasan penggunaan sistem AI;

(g) kecukupan ketelusan, langkah-langkah pengawasan manusia (*human oversight*) jika berkenaan; dan

(h) pelaksanaan tindakan pembetulan yang timbul daripada semakan, audit atau penilaian sebelumnya.

41.4 Jika berkenaan, log audit dan rekod lain yang berkaitan hendaklah disimpan dengan mengambil kira sifat pemprosesan dan potensi impak terhadap subjek data.

41.5 Dapatan daripada semakan dalaman atau audit dan apa-apa tindakan pembetulan yang diambil hendaklah didokumenkan dan disimpan dengan sewajarnya sebagai sebahagian daripada rekod akauntabiliti pengawal data.

41.6 Sekiranya semakan atau audit mengenal pasti kelemahan material, ketidakpatuhan atau risiko yang boleh menjejaskan data peribadi atau subjek data, pengawal data hendaklah mengambil langkah pembetulan yang bersesuaian dan memantau pelaksanaannya.

42. Pembuktian Pematuhan

42.1 Pengawal data hendaklah mampu menunjukkan bahawa pemprosesan data peribadi melalui sistem AI dijalankan selaras dengan Akta 709.

42.2 Pengawal data hendaklah menyelenggara bukti yang bersesuaian mengenai langkah-langkah yang dilaksanakan untuk melindungi data peribadi dan menyokong pematuhan terhadap Akta 709 berhubung penggunaan sistem AI.

42.3 Bukti tersebut boleh merangkumi, jika bersesuaian:

(a) dasar dan prosedur;

(b) rekod aktiviti pemprosesan yang melibatkan sistem AI;

(c) penilaian risiko dan Penilaian Impak Perlindungan Data, sekiranya dilaksanakan;

(d) rekod pengujian, semakan dan audit;

(e) keputusan tadbir urus dan kelulusan;

(f) rekod berkaitan dengan penyedia perkhidmatan AI;

(g) rekod insiden dan tindakan pembetulan; dan

(h) rekod latihan dan kesedaran.

43. Pengawasan Berterusan

43.1 Sekiranya penyedia perkhidmatan AI atau sistem AI luaran terlibat, pengawal data hendaklah mengekalkan pengawasan berterusan yang bersesuaian selaras dengan **Bahagian F** dan menyimpan rekod yang berkaitan mengenai pengawasan tersebut bagi menyokong pematuhan berterusan terhadap Akta 709.