**KERTAS KONSULTANSI AWAM BIL. 1/2015**

**CADANGAN STANDARD PERLINDUNGAN DATA PERIBADI**

1. **TUJUAN**

Kertas Konsultansi Awam Bilangan 1/2015 adalah bertujuan mendapatkan maklum balas daripada pengguna data dan subjek data berhubung kefahaman mengenai perlindungan data peribadi. Bagi menjadikan Standard Perlindungan Data Peribadi 2015 sebagai dokumen rujukan yang mantap, Pesuruhjaya Perlindungan Data Peribadi (Pesuruhjaya) telah bersetuju untuk menggabungkan ketiga-tiga standard iaitu Standard Keselamatan, Standard Penyimpanan dan Standard Integriti Data kepada satu dokumen yang konsisten. Langkah ini adalah selari dengan kehendak **Peraturan-Peraturan Perlindungan Data Peribadi 2013, Akta Perlindungan Data Peribadi 2010.**

Sehubungan dengan itu, maklum balas yang diterima melalui kertas konsultasi awam ini akan dianalisa dan hasil analisa tersebut akan digunakan dalam penyediaan draf akhir standard. Draf akhir tersebut juga akan dibentangkan kepada 11 golongan pengguna data sebelum didaftarkan oleh Pesuruhjaya.

1. **LATAR BELAKANG**

Sejak Januari 2015, Pejabat Pesuruhjaya Perlindungan Data Peribadi telah melaksanakan lawatan pemantauan ke atas premis-premis pengguna data yang berdaftar. Hasil daripada lawatan tersebut, pelbagai maklum balas dan penemuan dikumpulkan untuk dijadikan input bagi membangunkan standard minimum.

Bagi menjadikan standard ini mencukupi untuk mengawal selia pengguna data di Malaysia, Pesuruhjaya telah berkerjasama dengan Jabatan Standard Malaysia dan CyberSecurity Malaysia serta mengambil kira pandangan pakar dan juga amalan-amalan terbaik di peringkat antarabangsa.

Selain itu, Jawatankuasa Khas di peringkat Jabatan Perlindungan Data Peribadi yang diketuai oleh Timbalan Peusuruhjaya telah melaksanakan beberapa peringkat penilaian sebelum KERTAS KONSULTANSI AWAM BIL. 1/2015 ini diterbitkan.

1. **ARAHAN KEPADA PENGGUNA DATA DAN SUBJEK DATA**

Setiap Pengguna Data dan Subjek Data yang akan mengemukakan maklum balas dikehendaki:-

1. Membaca dengan teliti kandungan KERTAS KONSULTANSI AWAM BIL. 1/2015
2. Maklum balas konsultansi adalah seperti dalam **Lampiran A**
3. Cetak Lampiran A dan berikan maklum balas anda
4. Hantarkan maklum balas anda ke alamat berikut :

**KERTAS KONSULTANSI AWAM BIL. 1/2015**

**Aras 6, Kompleks KKMM, Lot 4G9,**

**Jabatan Perlindungan Data Peribadi**

**Kementerian Komunikasi dan Multimedia Malaysia**

**Persiaran Perdana, Presint 4,**

**Pusat Pentadbiran Kerajaan Persekutuan,**

**62100 Putrajaya.**

1. Kertas konsultansi tersebut juga boleh dihantar **melalui e-mel:** **mastura@pdp.gov.my** **atau** melalui **fax di talian: 603-89117959**
2. Tarikh akhir bagi menghantar maklum balas anda adalah pada **27 JULAI 2015 (ISNIN)**
3. **PENGHARGAAN**

Jabatan Perlindungan Data Peribadi (JPDP) dan Pesuruhjaya merakamkan penghargaan dan jutaan terima kasih di atas maklum balas yang dikemukakan.

-------t.t--------

**(MAZMALEK MOHAMAD)**

**Pesuruhjaya Perlindungan Data Peribadi Malaysia**

**LAMPIRAN A:**

**KERTAS KONSULTANSI AWAM BIL. 1/2015**

**BAHAGIAN 1- MAKLUMAT UMUM**

1. **Entiti : Pengguna Data/Subjek Data/Pengeluar Lesen Industri**
2. **Industri : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**BAHAGIAN 2- MAKLUM BALAS**

1. **PEMAKAIAN**

|  |  |
| --- | --- |
| **Bil.** | **Perkara** |
| 1 | Standard ialah suatu kehendak minimum yang dikeluarkan oleh Pesuruhjaya, bagi kegunaan biasa dan berulang, kaedah-kaedah, garis panduan atau ciri-ciri bagi aktiviti atau keputusan aktiviti itu, yang matlamatnya adalah pencapaian peringkat susunan yang optimum dalam sesuatu konteks yang diberikan. |
| 2 | Standard Perlindungan Data Peribadi ini terpakai kepada Pengguna Data yang **tidak berdaftar** dengan Pesuruhjaya. |
| 3 | Standard Perlindungan Data Peribadi ini terpakai bagi Golongan Pengguna Data **yang berdaftar** dengan Pesuruhjaya. |
| 4 | Standard Perlindungan Data Peribadi ini hendaklah dibaca bersama dengan **Kod** **Tata Amalan bagi Golongan Pengguna Data** yang didaftarkan oleh Pesuruhjaya. |
| 5 | Standard Perlindungan Data Peribadi ini berkuatkuasa **serta merta dari tarikh Akta Perlindungan Data Peribadi 2010** **dikuatkuasakan.** |
| 6 | **Maklum balas keseluruhan:** |

1. **STANDARD KESELAMATAN**

|  |
| --- |
| **PENGURUSAN DATA PERIBADI SECARA ELETRONIK** |
| **Bil.** | **Perkara** | **Komen** |
| 1 | Staf yang menguruskan data peribadi pelanggan perlu didaftarkan dalam satu sistem pendaftaran yang efisien sebelum diberi kebenaran mengakses ke sistem data peribadi pengguna |  |
| 2 | Kata laluan bagi suatu akaun user ID perlu ditukar apabila staf yang menggunakan ID tersebut tidak lagi menguruskan data peribadi pelanggan atau tidak lagi bekerja di organisasi tersebut dalam tempoh tiga (3) hari bekerja. |  |
| 3 | Sebelum staf berkenaan dibolehkan mengakses kepada sistem data peribadi, organisasi perlu menetapkan batas kuasa (*authorisation)* untuk setiap aktiviti memproses data peribadi supaya data hanya diproses untuk aktiviti yang berkaitan sahaja. |  |
| 4 | Pembatalan kebenaran akses perlu dilaksanakan apabila staf yang diberi *Unique* ID tidak lagi bekerja di organisasi tersebut dalam tempoh tiga (3) hari bekerja.  |  |
| 5 | Log Penggunaan Sistem perlu diselenggara dengan sempurna setiap minggu. Ini perlu dilaksanakan bagi mengawal selia akses kepada data peribadi pelanggan. |  |
| 6 | Pemindahan data peribadi secara elektronik hendaklah mematuhi prinsip-prinsip perlindungan data peribadi dan mempunyai Prosedur Operasi Standard (SOP) yang jelas dan teratur. |  |
| 7 | Parameter kawasan pemprosesan data peribadi pelanggan hendaklah berada di lokasi yang bersesuaian iaitu selamat daripada ancaman fizikal dan ancaman semulajadi. |  |
| 8 | Pengguna Data perlu menetapkan perimeter keselamatan fizikal seperti yang berikut:1. kawalan pergerakan keluar dan masuk

 ke tempat penyimpanan data (*entry*  *control*);1. menyediakan kamera litar tertutup di

 tempat penyimpanan data (sekiranya  perlu), dan1. menyediakan kawalan keselamatan

(*securing facilities*) 24 jam sehari (sekiranya perlu). |  |
| 9 | Pengguna Data perlu mempunyai *Back up/Recovery System* dan perisian anti-virus terkini bagi melindungi data pelanggan sekiranya berlaku insiden pencerobohan dan sebagainya. |  |
| 10 | Pengguna Data adalah dikehendaki membuat kawalan ke atas *malware* serta mengimbas sistem operasi komputer secara berjadual bagi mengelakkan serangan ke atas data yang disimpan secara elektronik. |  |
| 11. | Pemindahan Data Peribadi yang diproses secara elektronik perlu disekat kecuali dengan kebenaran pegawai yang diberi kuasa untuk aktiviti yang berkaitan sahaja. |  |
| 12 | Suatu kontrak perlu diadakan dengan pihak pemproses data (pihak ketiga) yang menjalankan aktiviti pemprosesan data peribadi bagi pihak pengguna data. Ini bagi maksud menjamin keselamatan ke atas data peribadi daripada kehilangan, salah guna, ubah suaian, akses dan penzahiran tanpa kebenaran. |  |
| **13** | **Maklum balas keseluruhan:** |

|  |
| --- |
| **PENGURUSAN DATA PERIBADI SECARA KONVENSIONAL** |
| **Bil.** | **Perkara** | **Komen** |
| 1 | Staf yang menguruskan data peribadi pelanggan perlu didaftarkan dalam satu sistem pendaftaran yang efisyen sebelum mengakses data peribadi pelanggan. |  |
| 2 | Rekod kebenaran mengakses data peribadi tersebut perlu disediakan dan diuruskan oleh Pengguna Data. |  |
| 3 | Pengguna Data perlu membatalkan kebenaran untuk akses data kepada staf yang tidak lagi terlibat dalam aktiviti memproses data peribadi pelanggan sama ada telah berpindah atau tidak lagi bekerja di organisasi Pengguna Data tersebut dalam tempoh tiga (3) hari bekerja. |  |
| 4 | Pengguna Data perlu menetapkan perimeter keselamatan fizikal di premis Pengguna Data seperti yang berikut:1. semua data peribadi disimpan secara

 teratur dalam fail;1. semua fail tersebut hendaklah

 disimpan di dalam kabinet berkunci  dan di dalam sebuah bilik yang  berkunci;1. semua kunci yang berkaitan

hendaklah disimpan di tempat yang selamat;1. hanya seorang sahaja yang diberi

kuasa untuk memegang kunci berkaitan. Manakala kunci pendua  hendaklah disimpan di tempat yang difikirkan selamat dan munasabah,  dan1. Tempat penyimpanan data peribadi

pelanggan hendaklah di lokasi yang bersesuaian iaitu selamat daripada ancaman fizikal atau semulajadi. |  |
| 5 | Pengguna Data perlu mengemaskini kebenaran mengakses data secara berkala bagi mengawal dan mengelakkan pengaksesan data peribadi oleh staf yang tidak diberi kuasa secara sah. |  |
| 6 | Pengguna Data perlu menyediakan Surat Aku Janji Kerahsiaan Data Peribadi Pelanggan untuk ditandatangani oleh setiap staf yang terlibat dengan data peribadi pelanggan. |  |
| 7 | Pengguna Data boleh mengadakan program kesedaran mengenai tanggungjawab melindungi data peribadi kepada semua staf sekiranya perlu. |  |
| 8 | Pemindahan data peribadi secara bukan konvensional hendaklah mematuhi prinsip-prinsip perlindungan data peribadi dan mempunyai Prosedur Operasi Standard (SOP) yang jelas dan teratur. |  |
| 9 | Semua kertas terpakai, dokumen cetakan atau lain-lain dokumen yang jelas menunjukkan data peribadi pelanggan perlu dimusnahkan dengan teliti dan efisien seperti menggunakan mesin rincih (*shredding machine*) atau lain-lain kaedah yang bersesuaian. |  |
| **10** | **Maklum balas keseluruhan:** |

1. **STANDARD PENYIMPANAN**

|  |
| --- |
| Pengguna data perlu mengambil langkah yang munasabah untuk memastikan bahawa segala data peribadi pelanggan dimusnahkan atau dipadamkan secara kekal. Jika data peribadi itu tidak lagi dikehendaki bagi maksud yang baginya data peribadi itu hendak diproses dengan: |
| **Bil.** | **Perkara** | **Komen** |
| 1 | Menentukan semua akta yang berkaitan dengan pemprosesan dan penyimpanan data peribadi sebelum memusnahkan data peribadi tersebut. |  |
| 2 | Melupuskan data peribadi dalam tempoh tidak melebihi tujuh (7) hari sebaik sahaja keperluan semua akta yang berkaitan telah dipenuhi. |  |
| 3 | Melupuskan data peribadi pelanggan dalam tempoh tidak melebihi tujuh (7) hari dari tarikh lengkap tamatnya transaksi komersial, jika transaksi itu tidak tertakluk di bawah mana-mana peruntukan perundangan untuk menyimpan data peribadi tersebut bagi suatu tempoh tertentu. |  |
| 4 | Menyelia dan melaporkan secara berkesan mengenai proses pemusnahan data peribadi tersebut. |  |
| 5 | Melupuskan borang pungutan data peribadi ketika pengambilan data peribadi untuk transaksi komersial dalam tempoh tidak melebihi tujuh (7) hari. |  |
| 6 | Melupuskan semua data peribadi yang tidak diperlukan dalam pangkalan data. |  |
| 8 | Mempunyai Prosedur Operasi Standard (SOP) bertulis mengenai pengeluaran semula data peribadi dari tempat penstoran sistem. |  |
| 9 | Mempunyai Prosedur Operasi Standard (SOP) bertulis mengenai kawalan keselamatan yang menyuluruh termasuk penyelenggaraan sistem dan penstoran sistem. |  |
| 10 | Mempunyai jadual berkala penghapusan data peribadi tidak aktif yang diselenggara dengan sempurna dan mempunyai rekod terhadap penyelenggaraan tersebut. |  |
| **HAL-HAL LAIN** |
| 11 | Bagi kawalan keselamatan, penggunaan *pendrive* atau *external hard disk* adalah tidak dibenarkan dilakukan secara sewenang-wenangnya tanpa kebenaran bertulis. |  |
| 12 | Penggunaan *pendrive* atau *external hard disk* untuk tujuan pengurusan data peribadi serta pengurusan dan pentadbiran sistem berkaitan mestilah mendapat kebenaran bertulis daripada pihak pengurusan atasan dan direkodkan. |  |
| **13** | **Maklum balas keseluruhan:** |

1. **STANDARD INTEGRITI DATA**

|  |
| --- |
| **PENGURUSAN DATA PERIBADI SECARA ELETRONIK** |
| Pengguna data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini dengan mengambil kira maksud, termasuk apa-apa maksud yang berhubungan secara langsung, yang baginya data peribadi itu dikumpulkan dan diproses selanjutnya. Langkah-langkah tersebut adalah: |
| **Bil.** | **Perkara** | **Komen** |
| 1 | Menyediakan borang kemaskini data peribadi untuk diisi oleh pelanggan. |  |
| 2 | Mengemaskini data peribadi dalam tempoh tidak melebihi tujuh (7) hari setelah mendapat notis pembetulan data peribadi daripada pelanggan. |  |
| 3 | Menentukan dokumen sokongan yang tepat dalam menentukan kesahihan data peribadi pelanggan.  |  |
| 4 | Memaklumkan kepada pelanggan melalui portal secara berjadual mengenai notis pengemaskinian data peribadi pelanggan. |  |
| 5 | Mempamerkan pemakluman jadual pengemaskinian data peribadi pelanggan di premis perniagaan. |  |
| 6 | Memaklumkan mengenai pengemaskinian tersebut pada masa-masa yang sesuai dalam tempoh yang sesuai dan dengan kaedah yang sesuai. |  |
| **PENGURUSAN DATA PERIBADI SECARA KONVENSIONAL** |
| Pengguna data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini dengan mengambil kira maksud, termasuk apa-apa maksud yang berhubungan secara langsung, yang baginya data peribadi itu dikumpulkan dan diproses selanjutnya. Langkah-langkah tersebut adalah: |
| 1 | Menyediakan borang kemaskini data peribadi untuk diisi oleh pelanggan. |  |
| 2 | Mengemaskini data peribadi dalam tempoh tidak melebihi tujuh (7) hari setelah mendapat notis pembetulan data peribadi daripada pelanggan. |  |
| 3 | Menentukan dokumen sokongan yang tepat dalam menentukan kesahihan data peribadi pelanggan. |  |
| 4 | Mempamerkan notis pengemaskinian data peribadi pelanggan secara berjadual di tempat yang bersesuaian di premis pengguna data. |  |
| 5 | Mempamerkan pemakluman jadual pengemaskinian data peribadi pelanggan di premis perniagaan. |  |
| 6 | Memaklumkan mengenai pengemaskinian tersebut pada masa-masa yang sesuai dalam tempoh yang sesuai dan dengan kaedah yang sesuai kepada pelanggan. |  |
| **7** | **Maklum balas keseluruhan:** |  |

**\*\*\*\*\*KERTAS KONSULTANSI TAMAT\*\*\*\*\***