Bar Malaysia
Malaysian Bar

www.malaysianbar.org.my

15 Leboh Pasar Besar
50050 Kuala Lumpur, Malaysia
Tel : +603-2050 2050
Fax : +603-2026 1313, 2034 2825, 2072 5818
Email : council@malaysianbar.org.my

Please note that you may submit your feedback to the email address or fax number provided in the circular below.

Circular No 160/2015
Dated 11 Aug 2015

To Members of the Malaysian Bar

Request for Feedback | Revised Personal Data Protection Standards

The Personal Data Protection Department ("PDP Department") had on 1 July 2015 issued the Public Consultation Paper No 1/2015 on the proposed Personal Data Protection Standards ("Standards").

Subsequently, the PDP Department has recently revised the Standards, as attached.

In this regard, the PDP Department invites Members of the Bar to provide feedback on the attached Revised Standards by **18 Aug 2015 (Tuesday)**.

Members of the Bar are encouraged to provide their feedback, by completing the attached Revised Standards, by email to Mastura bt Abd Rahim at mastura@pdp.gov.my, or by fax at 03-8911 7959. Feedback can also be sent by post, directly to:

The Commissioner of Personal Data Protection Malaysia
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
(Berkenaan: Cadangan Standard Perlindungan Data Peribadi)

Should you require any clarification, please contact Sarah Yong, Officer, by telephone at 03-2050 2093 or by email at sarah@malaysianbar.org.my.

Thank you.

Suaran Singh and Foong Cheng Leong
Co-Chairpersons
Ad Hoc Committee on Personal Data Protection

CADANGAN STANDARD PERLINDUNGAN DATA PERIBADI

A. 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 terpakai kepada Pengguna Data yang **berdaftar dan tidak berdaftar** dengan Pesuruhjaya.
3	Standard Perlindungan Data Peribadi ini hendaklah dibaca bersama dengan **Kod Tata Amalan bagi Golongan Pengguna Data** yang didaftarkan oleh Pesuruhjaya.
4	Standard Perlindungan Data Peribadi ini berkuatkuasa **serta merta daripada tarikh standard ini dikeluarkan.**

B. STANDARD KESELAMATAN

PENGURUSAN DATA PERIBADI SECARA ELETRONIK		
Bil.	**Perkara**	**Komen**
1	Organisasi yang menguruskan data peribadi pelanggan hendaklah didaftarkan dalam satu sistem pendaftaran pengguna data.	
2	Hak akses semua kakitangan kepada sistem data peribadi hendaklah ditamatkan selepas berhenti kerja, diberhentikan kerja, ditamatkan kontrak atau perjanjian, atau diselaraskan mengikut perubahan dalam organisasi.	
3	Organisasi dibolehkan mengakses kepada sistem data peribadi dan hendaklah menghadkan takat kuasa mengakses data peribadi kepada tujuan berkaitan sahaja.	
4	Log Penggunaan Sistem perlu diselenggara dengan sempurna dan hendaklah	

	dikemukakan apabila diarahkan oleh Pesuruhjaya.	
5	Organisasi hendaklah memastikan keselamatan pemindahan data peribadi secara elektronik selaras dengan Prinsip Keselamatan di bawah Akta 709.	
6	Lokasi pemprosesan data peribadi pelanggan hendaklah berada di tempat yang selamat daripada sebarang ancaman fizikal dan semulajadi.	
7	Pengguna Data perlu menetapkan prosedur keselamatan fizikal seperti yang berikut: i. kawalan pergerakan keluar dan masuk ke tempat penyimpanan data; ii. menyediakan kamera litar tertutup di tempat penyimpanan data (sekiranya perlu), dan iii. menyediakan kawalan keselamatan 24 jam sehari (sekiranya perlu).	
8	Pengguna data perlu mempunyai *Back up/Recovery System* dan perisian anti-virus yang sentiasa dikemaskini bagi melindungi data pelanggan daripada insiden pencerobohan dan sebagainya.	
9	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.	
10	Pemindahan data peribadi yang diproses secara elektronik adalah tidak dibenarkan kecuali dengan kebenaran bertulis pegawai yang diberi kuasa.	
11	Suatu kontrak perlu diadakan dengan pihak yang dilantik bagi 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.	

PENGURUSAN DATA PERIBADI SECARA KONVENSIONAL		
Bil.	**Perkara**	**Komen**
1	Organisasi yang menguruskan data peribadi pelanggan hendaklah didaftarkan dalam satu sistem pendaftaran.	
2	Hak akses semua kakitangan kepada sistem data peribadi hendaklah ditamatkan selepas berhenti kerja, diberhentikan kerja, ditamatkan kontrak atau perjanjian, atau diselaraskan mengikut perubahan dalam organisasi.	
3	Organisasi dibolehkan mengakses kepada sistem data peribadi dan hendaklah menghadkan takat kuasa mengakses data peribadi kepada tujuan berkaitan sahaja.	
4	Pengguna Data perlu menetapkan prosedur keselamatan fizikal seperti yang berikut: i. semua data peribadi disimpan secara teratur dalam fail; ii. semua fail tersebut hendaklah disimpan di dalam kabinet berkunci dan di dalam sebuah bilik yang berkunci; iii. semua kunci yang berkaitan hendaklah disimpan di tempat yang selamat; iv. hanya seorang sahaja yang diberi kuasa untuk memegang kunci berkaitan. Manakala kunci pendua hendaklah disimpan di tempat yang difikirkan selamat dan munasabah, dan v. Tempat penyimpanan data peribadi	Isu: klinik swasta dan pengamal undang-undang akan mengalami kesukaran selain melibatkan kos pematuhan yang tinggi. Isu: Banyak pihak tidak bersetuju hanya seorang diberi kuasa memegang kunci.

	pelanggan hendaklah di lokasi yang bersesuaian iaitu selamat daripada ancaman fizikal atau semulajadi.	
5	Rekod akses data peribadi perlu diselenggara dengan sempurna dan hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya.	
6	Organisasi perlu menyediakan Surat Aku Janji Kerahsiaan Data Peribadi Pelanggan untuk ditandatangani oleh setiap organisasi yang terlibat dengan data peribadi pelanggan.	Cadangan: perlu ditambah dalam elektronik
7	Pengguna data perlu mengadakan program kesedaran mengenai tanggungjawab melindungi data peribadi kepada semua yang terlibat.	Cadangan 1: Organisasi perlu mengemukakan laporan kepada Pesuruhjaya sekiranya mengadakan program kesedaran. Cadangan 2: Klaus ini dikeluarkan daripada standard kerana dikhuatiri akan membebankan pengguna data. Program ini boleh dilaksanakan bagi yang berkemampuan.
8	Pemindahan data peribadi secara konvensional seperti melalui pos, serahan tangan, faks dan sebagainya hendaklah mematuhi Prinsip Keselamatan di bawah Akta 709.	
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.	

C. 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 perundangan yang berkaitan dengan pemprosesan dan penyimpanan data peribadi sebelum memusnahkan data peribadi tersebut.	
2	Tidak menyimpan data peribadi lebih lama daripada yang diperlukan melainkan terdapat peruntukan undang-undang lain yang memerlukan penyimpanan data peribadi lebih lama.	
3	Set data peribadi yang berbeza hendaklah disimpan di tempat yang berlainan mengikut spesifikasi dan tujuan data.	
4	Rekod pelupusan data peribadi perlu diselenggara dengan sempurna dan hendaklah dikemukakan apabila diarahkan oleh Pesuruhjaya.	
5	Borang pungutan data peribadi untuk tujuan transaksi komersial hendaklah dilupuskan dalam tempoh tidak melebihi tujuh (7) hari melainkan borang pungutan data peribadi tersebut mempunyai nilai perundangan dan mempunyai kaitan dengan transaksi komersial tersebut.	
6	Melupuskan semua data peribadi yang tidak diperlukan dalam pangkalan data.	
7.	Mempunyai Prosedur Operasi Standard (SOP) bertulis mengenai pengeluaran semula data peribadi dari tempat penstoran sistem.	Cadangan 1: Dicadangkan digugurkan kerana dikhuatiri membebankan pengguna data untuk mengadakan SOP spesifik semata-mata untuk pengeluaran semula data peribadi dari tempat penstoran.
8	Mempunyai Prosedur Operasi Standard (SOP) bertulis mengenai kawalan	Cadangan 1: Dicadangkan digugurkan kerana dikhuatiri membebankan

	keselamatan yang menyeluruh termasuk penyelenggaraan sistem dan penstoran sistem.	pengguna data untuk mengadakan SOP spesifik berkenaan kawalan keselamatan.
9	Mempunyai jadual berkala penghapusan data peribadi tidak aktif yang diselenggara dengan sempurna dan mempunyai rekod terhadap penyelenggaraan tersebut.	
HAL-HAL LAIN		
10	Bagi kawalan keselamatan, penggunaan apa-apa peranti pemindahan data peribadi adalah tidak dibenarkan tanpa kebenaran bertulis daripada pegawai yang bertanggungjawab.	Cadangan 1: Semua transaksi pemindahan data peribadi melibatkan semua jenis kemudahan komunikasi hendaklah dilindungi.
11	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.	Cadangan 1: Dikeluarkan kerana sama di para 10

D. STANDARD INTEGRITI DATA

Pengguna data hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini dengan mengambilkira 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 secara bertulis untuk diisi oleh pelanggan sama ada secara konvensional atau elektronik.	
2	Mengemaskini data peribadi dalam tempoh tidak lewat dari dua puluh satu (21) hari setelah mendapat notis pembetulan data peribadi daripada subjek data.	
3	Menentukan dokumen sokongan yang tepat dalam menentukan kesahihan data peribadi subjek data.	

4	Memaklumkan kepada pelanggan melalui portal secara berjadual mengenai notis pengemaskinian data peribadi pelanggan.	Cadangan 1: Digugurkan kerana perkara ini boleh dimasukkan dalam COP
5	Mempamerkan pemakluman jadual pengemaskinian data peribadi pelanggan di premis perniagaan.	Cadangan 1: Digugurkan kerana perkara ini boleh dimasukkan dalam COP
6	Memaklumkan mengenai pengemaskinian tersebut pada masa-masa yang sesuai dalam tempoh yang sesuai dan dengan kaedah yang sesuai.	Cadangan 1: Digugurkan kerana perkara ini boleh dimasukkan dalam COP