KERTAS CADANGAN

[No. 2/2014]

"PANDUAN PEMATUHAN AKTA PERLINDUNGAN DATA PERIBADI (PDPA) 2010"

Jabatan Perlindungan Data Peribadi mengalu-alukan maklum balas dan pendapat secara bertulis kepada Jabatan berhubung dengan perkara yang dibangkitkan di dalam kertas ini. Maklum balas dan pendapat hendaklah dikemukakan sebelum 20 Mac 2014 kepada alamat atau e-mel seperti berikut:-

Pesuruhjaya Perlindungan Data Peribadi Malaysia
Aras 6, Kompleks KKMM
Lot 4G9, Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya
Emel: pcpdp@pdp.gov.my
Faks: 03 8911 7959

Pegawai untuk dihubungi –

Siti Dinar binti Othman (Tel: 03 8911 7924)
Sengngeng binti Mohd. Saleng (Tel: 03 8911 7397)
Ahmad Syazwan bin Mohd Ghazali (Tel: 03 8911 7920)

Kertas ini bertujuan untuk mendapatkan maklum balas dan pendapat berkenaan cadangan Jabatan Perlindungan Data Peribadi (Jabatan) untuk mewujudkan Panduan Pematuhan Akta Perlindungan Data Peribadi (APDP) 2010

Akta Perlindungan Data Peribadi telah diluluskan oleh Parlimen pada bulan Mei 2010. Akta ini menandakan satu pencapaian penting bagi Malaysia dalam merapatkan jurang antara undang-undang Malaysia dan *trend* antarabangsa berkaitan dengan perlindungan data peribadi. Akta memperkatakan tentang pemprosesan yang meliputi pengumpulan, penggunaan, penyimpanan dan penzahiran data peribadi daripada mana individu boleh dikenal pasti. Ia terpakai secara konsisten kepada semua jenis data peribadi, tanpa mengira tahap sensitiviti.

2. Memandangkan skop aplikasi undang-undang ini yang luas, banyak organisasi, daripada pemilikan tunggal dan syarikat kecil dan sederhana hinggalah kepada syarikat multinasional dikehendaki mengambil langkah-langkah yang perlu untuk mewujudkan, mengkaji semula dan memperkukuhkan polisi dalaman, prosedur, proses dan sistem yang melaksanakan pengurusan dan pengendalian data peribadi bagi mematuhi undang-undang ini. Ini amat perlu dilakukan memandangkan Akta ini

merangkumi organisasi yang memproses data peribadi secara harian sebagai contoh, antaranya syarikat telefon, syarikat perbankan dan insurans, perkhidmatan profesional dan firma pengambilan pekerjaan.

Cara Pematuhan Akta

3. Garis panduan ini disediakan sebagai senarai semak yang boleh digunakan oleh entiti pemprosesan data peribadi atau organisasi untuk mematuhi Akta.

3.1. Pendaftaran Sebagai Pengguna Data

Organisasi perlu menyemak Perintah Menteri berkaitan yang diwartakan pada November 2013 untuk menentukan sama ada dikehendaki berdaftar dengan Pesuruhjaya / Jabatan Perlindungan Data Peribadi (JPDP). Maklumat lanjut berkenaan perkara ini boleh dilayari di www.pdp.gov.my. Tujuan pendaftaran, selain untuk ketelusan; adalah untuk membolehkan organisasi mengambil bahagian dalam pelbagai forum industri yang akan ditubuhkan dan yang bertanggungjawab dalam merumus kod tataamalan untuk pematuhan. Namun demikian, perlu diambil perhatian bahawa semua organisasi, sama ada yang perlu berdaftar atau tidak; yang berurusan dengan data peribadi dalam konteks transaksi komersil hendaklah mematuhi undang-undang ini.

3.2. Tanggungjawab Berkaitan Perlindungan Data Peribadi

Bagi membantu pematuhan, adalah penting bagi setiap organisasi untuk meletakkan tanggungjawab berhubung dengan perlindungan data peribadi di peringkat tertinggi dan menetapkan pegawai untuk melaksanakan tanggungjawab tersebut. Pegawai yang dilantik akan bertanggungjawab untuk memastikan semua polisi, prosedur, sistem dan operasi adalah sejajar dengan tuntutan Akta. Sumber yang diperlukan bagi pelaksanaan ini akan bergantung kepada pelbagai faktor termasuk saiz data peribadi termasuk data peribadi pekerja, vendor dan pelanggan dikendalikan atau diuruskan oleh organisasi. Bagi organisasi yang lebih besar, pasukan petugas mungkin perlu ditubuhkan untuk menjaga pengendalian data peribadi dari perspektif pelan pengurusan strategik.

3.3. Aspek Operasi Data Peribadi

Sebagai permulaan, organisasi perlu mengenal pasti bidang operasi perniagaannya yang berurusan dengan pengendalian data peribadi serta semua polisi, kaedah dan peraturan bagi pengendaliannya. Pada ketika ini, mungkin wujud keperluan bagi organisasi melakukan analisa untuk menentukan status semasa organisasi dan langkah-langkah yang perlu diambil untuk mematuhi Akta. Dalam konteks ini, organisasi perlu menilai semula polisi-polisi yang sedia ada dan kaedah pemprosesan data, dengan

tujuan untuk membuat penambahbaikan dan pelarasan bagi disesuaikan dengan tuntutan Akta. Beberapa aspek utama yang perlu diberi perhatian dalam membuat penilaian di atas termasuk sumber pengumpulan data peribadi, aktiviti pengumpulan, prosedur akses dan pembetulan, penyimpanan dan keselamatan sistem serta aktiviti penzahiran.

3.4. Langkah Seterusnya

Antara pelan tindakan yang boleh dipertimbangkan sebagai panduan hala tuju bagi organisasi untuk menyesuaikan diri dengan keperluan Akta termasuk:

3.4.1 mempertimbangkan pelan keselamatan yang munasabah untuk menghalang capaian atau pengumpulan, penggunaan atau pendedahan data peribadi yang tidak dibenarkan dalam milikan organisasi;

3.4.2 memperkenalkan manual pematuhan / program yang mentakrifkan aliran kerja yang terlibat;

3.4.3 memastikan pelan tindakan tersedia bagi mengelakkan insiden penyalahgunaan data dengan mengambil langkah-langkah untuk mendapatkan persetujuan rasmi pelanggan, memberitahu subjek data mengenai pemprosesan data peribadi mereka dan mematuhi

permintaan untuk mengakses atau membetulkan data peribadi mereka;

3.4.4 meningkatkan kesedaran kakitangan dan menangani semua pertanyaan berkaitan polisi-polisi dan amalan-amalan perlindungan data peribadi organisasi melalui program latihan dalaman secara berkala;

3.4.5 menjalankan kajian terhadap terma dan syarat pekerjaan terutamanya dalam perkara-perkara yang berkaitan dengan hak dan kewajipan pekerja berkenaan dengan data peribadi seperti yang digariskan dalam Akta;

3.4.6 memastikan semua kontrak perkhidmatan dengan pihak ketiga atau pemproses luar meliputi langkah-langkah perlindungan dalam aspek kualiti, keselamatan, pematuhan dan pemeriksaan berkaitan dengan data peribadi.

3.4.7 memastikan pematuhan dengan obligasi yang berkaitan di bawah Akta bagi kedua-dua bidang kuasa import dan eksport dalam hal berkaitan pemindahan data peribadi rentas sempadan; dan

3.4.8 mengikuti perkembangan terkini di dalam perlindungan data peribadi di dalam negara termasuk garis panduan dan peraturan yang akan diperkenalkan oleh Jabatan dari semasa ke semasa.

Kertas di atas mewakili cadangan awal Jabatan. Oleh itu, Jabatan ini ingin mengalu-alukan sebarang maklum balas dan pendapat mengenai perkara-perkara yang dicadangkan.

PROPOSAL PAPER

[No. 2/2014]

"GUIDELINE ON COMPLIANCE OF PERSONAL DATA PROTECTION ACT (PDPA) 2010"

Personal Data Protection Department welcomes the feedback and opinion in writing to the Department in relation to matters raised in this paper. The feedback and opinion shall be submitted before 20 March 2014 to the address or e-mail as follows -

Personal Data Protection Department
Level 6, Kompleks KKMM
Lot 4G9, Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya
Email: pcpdp@pdp.gov.my
Fax: 03 8911 7959

Contact person –

Siti Dinar binti Othman (Tel: 03 8911 7924)
Sengngeng binti Mohd. Saleng (Tel: 03 8911 7397)
Ahmad Syazwan bin Mohd Ghazali (Tel: 03 8911 7920)

The paper seeks to obtain feedback and opinion on the proposal of the Personal Data Protection Department (the Department) to establish a Guideline on Compliance of Personal Data Protection Act (PDPA) 2010.

The Personal Data Protection Act was passed by Parliament in May 2010. The Act signals an important milestone for Malaysia in bridging the gap between Malaysia's laws and international trends in respect of personal data protection. The Act deals with the processing including collection, use, retention and disclosure of personal data from which an individual can be identified. It applies consistently across all types of personal data, regardless of the degree of sensitivity.

2. Given the wide scope of application of the law, many organizations, ranging from sole proprietors and small-to medium enterprises to multi-national corporations are required to take the necessary steps to establish, review and strengthen internal policies, procedures, processes and systems that govern the management and handling of personal data in order to comply with the law. This is especially so as the Act affects organisations which process personal data on a day-to-day basis for example, phone companies, bank and insurance companies, professional services and recruitment firms to mention a few.

How To Comply With The Act

3. This guideline has been established as possible check-list that could be used by the personal processing entities or organizations to comply with the Act.

3.1. **Registration As Data Users**

Organizations must check the relevant Minister Order gazetted in November 2013 to determine whether they are required to register with the Commission/Department Of Personal Data Protection (DPDP). They can log in at www.pdp.gov.my for further information on this. The purpose of registration, apart from transparency reason; is to enable organizations to participate in the various industry forums which will be established and responsible for the formulation of codes of practices for their compliance. Please take note that all organizations that deal with personal data in the context of commercial transactions are required to comply with the law irrespective of whether or not they are required to register.

3.2. **Responsibility Pertaining To Personal Data Protection**

To facilitate compliance, it would be vital for every organization to establish responsibility in relation to protection of personal data at the highest level

and designate an officer to discharge such responsibility. The said officer will be responsible for ensuring that all the policies, procedures, systems and operations are aligned to the requirements of the Act. The amount of resources required will depend on many factors including the size of personal data including of employees, vendors and clients being handled or dealt with by the organization. For larger organizations, it may be necessary for appropriate task force to be established to look after the handling of personal data from the perspective of strategic management plans.

3.3. **Operational Aspects Of Personal Data**

As a starting point, organizations should identify the areas of its business operations that deal with the management and handling of personal data as well as all policies, rules and regulations that govern them. It may be necessary at juncture that analysis be performed to determine the current status of the organization and measures needed to be taken in order to comply with the Act. In this context, organizations should reassess existing policies and data processing methods, with a view of making improvements and adjustments to align them with the Act. Some of the key aspects that must be given attention in making the above evaluation include sources of

personal data, collection practices, access and correction procedures, storage and security system and disclosure practices.

3.4. **Next Steps**

Among some of the action plans that could be considered as a roadmap for organizations to adjust to the requirements of the Act include:

3.4.1 considering reasonable security arrangements to prevent unauthorised access to or collection, use or disclosure of personal data in possession;

3.4.2 introducing compliance manual/programme which defines workflow involved;

3.4.3 ensuring measures are in place to prevent data breach by taking the steps to reach out to clients for obtain formal informed consent, notifying data subjects on the processing of their personal data and complying with requests for access or correction of personal data;

3.4.4 raising awareness and addressing all queries among staff on personal data protection policies and practices through conducting in-housing training programmes on regular basis;

3.4.5 undertaking review of the employment terms particularly on matters pertaining to the rights and obligations of employees in respect of personal data as outlined in the Act;

3.4.6 ensuring that all service contracts with third or outsourced parties processors cover quality, security, compliance and inspection safeguards and measures related to personal data.

3.4.7 ensuring compliance, for cross-border transfers of personal data; with relevant obligations under the Act on both import and export jurisdictions.

3.4.8 keeping abreast with latest developments in personal data protection of the country including the guidelines and rules that will be introduced by the Department from time to time.

The paper above represents initial suggestions of the Department. The Department would therefore like to welcome any feedback and opinion on the above proposed matters.