FIMM

3 March 2014

CIRCULAR : **LSRA/AL/MN-nh/009 -14**
(TOTAL NO. OF PAGE(S): 27)

TO :
i. MEMBERS, IUTA AND CUTA
ii. PRS PROVIDERS, INSTITUTIONAL PRS ADVISERS AND CORPORATE PRS ADVISERS

ATTN. : **AUTHORISED REPRESENTATIVE/CHIEF EXECUTIVE OFFICER**

FEEDBACK ON PROPOSAL PAPERS:
(i) 2/2014 - GUIDELINE ON COMPLIANCE OF PERSONAL DATA PROTECTION ACT (PDPA) 2010
(ii) 3/2014 - GUIDE ON THE MANAGEMENT OF EMPLOYEE DATA UNDER PERSONAL DATA PROTECTION ACT (PDPA) 2010

Your attention is brought to the above captioned matter.

The Personal Data Protection Department ("Department") is seeking feedback and opinion on the proposal papers mentioned above, which present the initial suggestions of the Department.

Please note that the Department has set **20 March 2014** as the closing date for submission. As such, we would appreciate it if you could provide your feedback and opinion in writing directly to the Department either by post, fax or e-mail to the address and number included in the proposal papers. A copy each of the proposal papers (in Bahasa Malaysia and English) is attached for your reference.

If you have any query, please contact Sharon Kaur (ext. 309) or Noraishah Hamid (ext. 302) of Legal, Secretarial & Regulatory Affairs at 03-2093 2600.

Yours faithfully,
Federation of Investment Managers Malaysia

MOHAMED NIZA B ABU BAKAR
Chief Executive Officer

Encls.

FEDERATION OF INVESTMENT MANAGERS MALAYSIA (272577-P)
(formerly known as Federation of Malaysian Unit Trust Managers)
19-07-3, 7th Floor PNB Damansara, No.19 Lorong Dungun, 50490 Kuala Lumpur
• T 603 2093 2600 • F 603 2093 2700 • www.fimm.com.my

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.

KERTAS CADANGAN

[No. 3/2014]

"PANDUAN PENGURUSAN DATA PEKERJA DI BAWAH AKTA PERLINDUNGAN DATA PERIBADI (APDP) 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 -

Jabatan Perlindungan Data Peribadi
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 Pengurusan Data Pekerja Di Bawah Akta Perlindungan Data Peribadi (APDP) 2010

Latar belakang

1. Dengan berkuatkuasanya Akta PDP dari 15 November 2013, majikan adalah dinasihatkan untuk mengkaji semula pendekatan dan kontrak yang berkaitan dengan pekerjaan termasuk penyediaan mekanisme dan proses yang perlu untuk mematuhi tujuh Prinsip Akta PDP.

Kenapa Akta PDP Terpakai Kepada Majikan-Pekerja

2. Baru-baru ini beberapa pertanyaan telah diterima oleh Jabatan yang inginkan penjelasan bagi pemakaian Akta PDP kepada hubungan majikan-pekerja. Ini adalah berdasarkan Seksyen 2 Akta yang memperuntukkan bahawa Akta hanya terpakai kepada mana-mana orang yang memproses dan mengawal pemprosesan data peribadi berkenaan dengan transaksi komersial. Di bawah Seksyen yang sama *"transaksi komerisal"* telah ditakrifkan dalam Akta sebagai *"apa-apa transaksi yang bersifat komersial, sama ada secara kontrak atau tidak, yang termasuk apa-apa perkara yang berhubungan dengan pembekalan atau pertukaran barang atau perkhidmatan, agensi, pelaburan, pembiayaan, perbankan dan insuran ... "*. Berdasarkan dengan takrif dan peruntukan di atas, ia adalah jelas bahawa hubungan majikan-pekerja adalah komersial dan bersifat kontraktual kerana ia timbul daripada kontrak perkhidmatan sebagai tukaran bagi upahan dan Akta PDP terpakai kepada hubungan tersebut.

Prinsip-prinsip Akta PDP

3. Dalam menguruskan dan mengendalikan data peribadi pekerja, majikan mesti mematuhi tujuh Prinsip Perlindungan Data Peribadi seperti yang ditetapkan dalam Akta. Prinsip-prinsip ini adalah seperti berikut:

a) Prinsip Am

Dengan prinsip di atas, majikan perlu mematuhi peraturan berikut :

i) mendapatkan persetujuan daripada pekerja apabila mengumpul data peribadi biasa; dan
ii) mendapatkan persetujuan yang nyata apabila mengumpul data peribadi yang sensitif.

Walau bagaimanapun, syarat-syarat untuk mendapatkan persetujuan berhubung dengan pengumpulan / pemprosesan data peribadi dikecualikan bagi tujuan pelaksanaan kontrak di mana pekerja itu merupakan suatu pihak di dalamnya. Ini bermakna bahawa untuk melayakkan pengecualian, majikan kini perlu menilai dan menentukan maklumat yang benar-benar perlu bagi memenuhi tugas dan tanggungjawab kedua-dua majikan dan pekerja bagi mengelakkan pengumpulan data yang berlebihan.

b) Prinsip Notis dan Pilihan

Di bawah prinsip ini majikan dikehendaki untuk memaklumkan pekerja:

i) jenis maklumat yang dikumpulkan;
ii) sama ada maklumat itu akan dikongsi dengan pihak ketiga; dan
iii) bahawa pekerja mempunyai hak untuk mengakses maklumat yang dikumpul. (ini adalah keperluan yang berasingan daripada keperluan persetujuan di bawah Prinsip Am)

c) Prinsip Penzahiran

Berhubung dengan Prinsip Penzahiran, semua majikan dinasihatkan supaya memberi lebih perhatian kepada aktiviti perkongsian data dengan pihak ketiga, khususnya dengan syarikat bersekutu atau syarikat-syarikat yang dimiliki oleh kumpulan majikan yang sama. Undang-undang memperuntukkan bahawa pengguna data tidak dibenarkan untuk berkongsi data dengan pihak ketiga melainkan jika persetujuan individu telah diperolehi. Ini juga melibatkan majikan yang menyumberkan fungsi tertentu Sumber Manusia kepada syarikat-syarikat luar*(outsourcing)* yang berkaitan dengan pekerjaan seperti gaji, kesihatan, pembiayaan dan latihan.

d) Prinsip Keselamatan

Akta PDP mengenakan peraturan yang lebih ketat berkaitan dengan aspek-aspek keselamatan dalam pemprosesan data peribadi. Oleh itu, majikan bertanggungjawab untuk memastikan bahawa langkah-langkah keselamatan yang secukupnya telah diambil untuk melindungi maklumat kakitangan dalam kawalannya. Aspek-aspek utama yang perlu diberi penekanan termasuk tempat dan lokasi penyimpanan, langkah-langkah keselamatan diaplikasikan ke dalam apa-apa perkakasan yang digunakan dan prosedur akses oleh kakitangan kepada data peribadi pekerja. Atas sebab praktikal, fail peribadi pekerja hendaklah disimpan di dalam kabinet berkunci dengan selamat. Dalam aktiviti penyumberan fungsi-fungsi Sumber Manusia ke luar(outsourcing), majikan juga bertanggungjawab untuk memastikan bahawa pihak ketiga yang berkenaan mengambil langkah yang munasabah dalam melindungi data peribadi.

e) Prinsip Penyimpanan

Dalam Prinsip Penyimpanan, majikan perlu mengambil langkah-langkah untuk memusnahkan data peribadi apabila data itu didapati tidak lagi diperlukan bagi maksud awal pemprosesannya. Persetujuan baru hendaklah diperolehi daripada pekerja berkenaan sekiranya majikan perlu menyimpan data peribadi itu untuk tujuan lain termasuk bagi kegunaan masa depan. Walau bagaimanapun, majikan perlu turut prihatin terhadap kewajipan tertentu yang dikenakan oleh undang-undang lain bagi

mengekalkan data pekerjanya walaupun selepas tamat penggajian. Sebagai contoh, Seksyen 61 Akta Kerja 1955 yang menuntut majikan untuk menyimpan daftar maklumat pekerja untuk tempoh tidak kurang daripada enam tahun. Kos pematuhan termasuk risiko keselamatan yang berkaitan boleh dikurangkan jika majikan hanya mengumpul dan menyimpan data peribadi yang diperlukan untuk tujuan perniagaan mereka dan memadam atau *anonymize* data peribadi yang tidak lagi diperlukan.

f) Prinsip Integriti Data

Undang-undang ini mengenakan kewajipan kepada majikan untuk mengambil langkah yang perlu bagi memastikan bahawa semua data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini. Sebagai amalan yang baik, majikan digalakkan untuk mengemaskini data peribadi pekerja secara berkala bagi memastikan data peribadi seperti adalah tepat dan terkini.

g) Prinsip Akses

Sebagai peraturan, majikan mesti menyediakan kemudahan untuk membolehkan pekerja diberi akses kepada maklumat mereka bagi memudahkan proses pengemaskinian terutamanya dalam keadaan di mana terdapat apa-apa ketidaktepatan, maklumat yang tidak lengkap, maklumat yang mengelirukan atau maklumat tidak terkini. Majikan bagaimanapun diberi pengecualian kepada peraturan ini terutamanya dalam menangani keadaan tertentu seperti penglibatan unsur-unsur kerahsiaan.

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. 3/2014]

"GUIDE ON THE MANAGEMENT OF EMPLOYEE DATA UNDER 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 Guide on The Management of Employee Data Under Personal Data Protection Act (PDPA) 2010

Background

1. With the coming into force of the PDP Act effective from 15th of November 2013, employers are advised to revisit their approaches and contracts related to employment including putting in place the necessary mechanisms and processes to comply with the seven Principles of the PDP Act.

Why PDP Act Applies On Employer –Employee Relationship

2. Recently some enquiries have been received by the Department seeking clarification on whether the PDP Act applies to an employer–employee relationship. This is in light of Section 2 of the Act which provides that the Act only applies to any person who processes and has control over the processing of personal data in respect of commercial transactions. Under the same Section "*commercial transaction*" has been defined in the Act as *"any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of good or services, agency, investments, financing, banking and insurance…"*. Based on the above provision and definition, it is clear that employer-employee relationship is commercial and contractual in nature as it arises from a contract of services in exchange for remuneration and the *PDP Act applies to such a relationship.*

Principles Of The PDP Act

3. In managing and dealing with personal data of employee, employer must observe the seven Principles of Personal Data Protection as stipulated in the Act. These principles are as follows:

a) General Principle

With the above principle, employers must observe the following rules :

i) obtain *consent* from the employees when collecting normal personal data; and

ii) obtain *explicit consent* when collecting *sensitive personal data*.

However, the requirements to get consent in relation to personal data collecting/processing is *exempted* for the *performance of a contract* to which the employee is a party. This would mean that in order to qualify for exemption an employer must now evaluate and determine what information is absolutely necessary for the discharge of both the employer and employees' duties and obligations to avoid *excessive* data collection.

b) Notice and Choice Principle

Under this principle an employer is required to inform the employee:

i) the nature of the information collected;
ii) whether the information would be shared with a third party; and
iii) that the employee has the right to access the information collected. (this is separate requirement from consent requirement under the General Principle)

c) *Disclosure Principle*

With regard to the Disclosure Principle, all employers are advised to exercise extra care when it comes to matters pertaining to sharing of personal data with third parties, in particular the associate or sister companies that are belonging to the same group of employer. The law provides that a data user is not allowed to share data with third parties unless the consent of the individual is obtained. This would impact employers who outsource certain HR functions related to employment like payroll, health, financing and training to external outsourcing companies.

d) Security Principle

The law imposes stricter rules with regard to the security aspects in the processing of personal data. Employer is therefore

responsible for ensuring that adequate security measures are in place to protect the employees' information in its control. Key aspects that need to be given emphasis include the place and location of the storage, security measures incorporated into any equipment used as well as access procedures by personnel to personal data of the employees. For practical reason, employees' personal files should be kept in securely locked cabinets. Employer is also responsible for ensuring that, in a situation of outsourcing of HR functions; a third party concerned take reasonable steps to put in place security measures to protect the personal data.

e) Retention Principle

With the Retention Principle, employers must take measures to securely destroy the personal data whenever such data is found no longer required for the purpose for which it was processed. Fresh consent must be obtained from the employee concerned if the employer needs to retain such personal data for other purposes including future use. However, employers should be mindful of certain obligations imposed by other law on the requirement of retaining data of its employees even after the cessation of employment. For example, Section 61 of the Employment Act 1955 mandates employers to keep information registers of its employees for a period not less than six years. Compliance costs including the associated security risks can be reduced if employer only collect and retain personal data that is necessary for their business

purposes and delete or anonymize personal data when it is no longer necessary.

f) ***Data Integrity Principle***

The law imposes obligation on the part of employer to take the necessary measures to ensure that all personal data is accurate, complete, not misleading and kept up to date. As matter of good practices, employer is encouraged to update the personal data of employees on regular basis so as to ensure such personal data is up to date and accurate.

g) ***Access Principle***

As a rule, employer must provide the facility to enable employees to be given access to their information so as to facilitate the updating processes particularly in the event where there are any inaccuracies, incomplete information, misleading information or that the information is not up to date. Employer however is given exemption to this rule particularly in dealing with certain circumstances, such as where there is an element of confidentiality involved.

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.