



## **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](mailto: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 komersial*" 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 pemrosesan 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 pemrosesannya. 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 pekerjaanya walaupun selepas tamat pengajian. 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](mailto: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 15<sup>th</sup> 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.**