PDPA 2010 :

SOLUTION - FOCUSED QUESTIONS

PESURUHJAYA PERLINDUNGAN DATA PERIBADI MALAYSIA
Personal Data Protection Commissioner Malaysia

Notice

All the questions in this handbook are extracted and compiled from the Q&A sessions at the PDPA Seminars 2016

How are insurance agents / third parties be held responsible for the breach of PDPA?

If a data user clearly states in its contract with the third party the responsibilities for compliance to the PDPA when processing personal data on their behalf, any breach by the third party may subject them to fine/imprisonment or both.

We collect tourist data online when they book tour. Our website is hosted outside Malaysia, but processed in Malaysia. Should we be concerned with the data that is parked outside Malaysia?

Yes, you must ensure that there is in that place outside Malaysia in force any law which is substantially similar to the PDPA, or that serves the same purposes as the Act; or that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by PDPA.

Do we need consent from the judgement debtor / defendant regarding their data before we proceed to court or are we protected / included as the 3rd party in bank's agreement between bank and customer?

No, as you are included as the 3rd party in bank's agreement between bank and customer.

What is the scope of the PDPA when a tour operator collects information and must then pass it on to other suppliers in the chain, for example transport company, hotels and so on. If a data breach occurs in one of the suppliers, is the tour operator liable?

If a data user clearly states in its contract with the third party the responsibilities for compliance to the PDPA when processing personal data on their behalf, any breach by the third party may subject them to fine/imprisonment or both.

? In order to save cost, traceability, easier control and management, at the same time to comply with the PDPA requirements; can a data user scan a record to replace the original record? E.g.: Blood test request form

Yes, you may scan the records. However, as the records are sensitive data; you are to ensure that the security of the data is in accordance with the Security Principle and the PDP Standard.

? Can we send promotions via Facebook to our customers?

Yes. However, sending promotional newsletters or updates must be consented by your customers.

? Can we reveal the medical history of patients for the purpose of medical treatment for that particular patient?. For example, our medical centre reveals patients' medical history to government hospital.

As required by Section 40 of the PDPA, a data user shall not process any sensitive data of a data subject without his/her explicit consent. Nevertheless, with reference to your situation; Section 40(b)(iv) provides an exception with the condition that the processing is necessary for medical purposes and is undertaken by - (A) a healthcare professional; or (B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional.

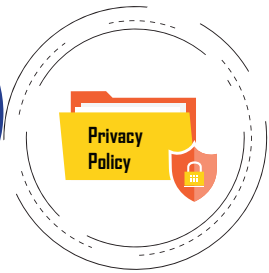
? As a data processor for cloud computing services, would there be a need to inform clients via a privacy notice of our services? Would a general privacy notice be sufficient? Do we need to obtain a specific consent for the transfer of data oversea?

A Privacy Notice which must be in line with all the provisions under Section 7, PDPA must be served by a **data user** to his/her customer upon processing customers' personal data. In addition, consent for the transfer of personal data oversea must also be obtained by a **data user**. Nevertheless, as a data processor; you are accountable to ensure the security of transfer.

? We have CCTV notices that inform data subjects are under 24 hours surveillance. Do we need to specifically state it is for security purpose on the notice? We have it spelled out in our company policy that the CCTV data is only used for security purpose.

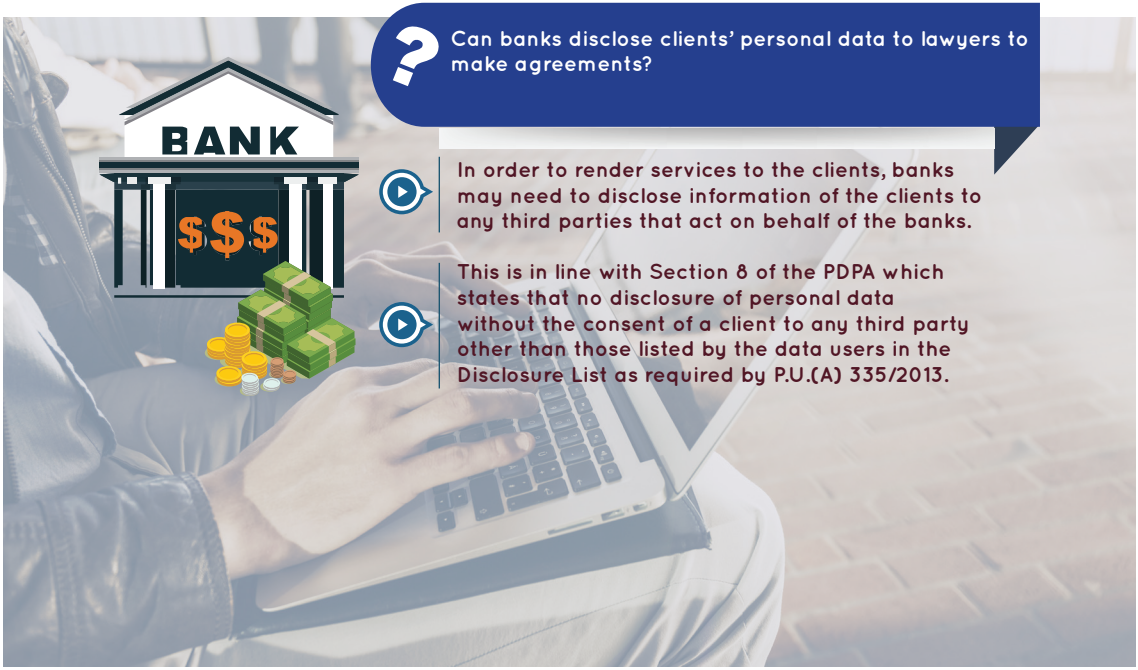
You may put up a simple CCTV notice of "Surveillance for Security".

? Is there a sample "Privacy Notice" for display at hotel reception counter? Currently many hotels do not display Privacy Notice at the reception counter. Maybe KKMM can communicate with MAH (Malaysia Associations of Hotels to provide us more guidance for implementation.



The Commissioner's Office has established a Guide on Privacy Notice. Yes, the Office has been communicating with MAH in coming up with the Code of Practice for Tourism & Hospitality Sector.

PRINSIP PENZAHIRAN
DISCLOSURE PRINCIPLE



Can banks disclose clients' personal data to lawyers to make agreements?

In order to render services to the clients, banks may need to disclose information of the clients to any third parties that act on behalf of the banks.

This is in line with Section 8 of the PDPA which states that no disclosure of personal data without the consent of a client to any third party other than those listed by the data users in the Disclosure List as required by P.U.(A) 335/2013.

Adakah perlu persetujuan khusus daripada subjek data untuk pengguna data menzahirkan dan membandingkan data di dalam sistem (tiada campur tangan manusia). Bagaimanakah jika salah satu daripada pengguna data adalah syarikat asing?

Prinsip Penzahiran APDP menetapkan bahawa tiada data peribadi subjek data boleh dizahirkan tanpa persetujuannya.

? The company currently sets the retention period for keeping personal data of resigned staff as 7 years. However, there are requests from HR to keep the personal file longer than 7 years. Is that okay? Do we, as the organisation need to inform the resigned staff that their personal data (the consent) form will be kept after the 7th year?

PDPA requires for any personal data processed to be kept no longer than necessary unless there are requirements by other legal provisions. A retention period that exceeds the requirements by other legal provisions will be detailed out in the Code of Practice of the related Class of Data User. The staff can be informed of the policy in their employment contract.

? Voice recording to obtain consent from customers. Is there a retention period for the digital recording?

Under P.U.(A) 335/2013, consent in whatever form must be able to be recorded and maintained and the burden of proof shall lie on the data user. On the retention period for digital recording, it is advisable for your company to include the retention period in the company's retention policy. The PDPA requires for any personal data processed to be kept no longer than necessary unless there are requirements by other legal provisions.

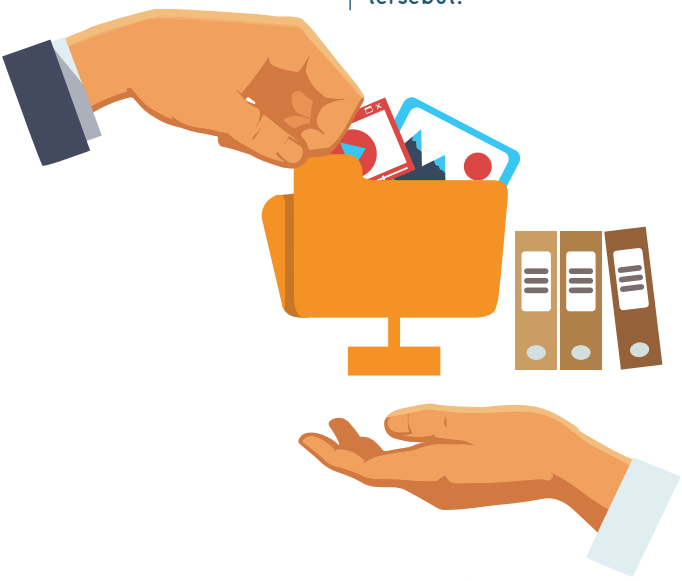
PRINSIP PENYIMPANAN
RETENTION PRINCIPLE

? Kami merupakan sebuah universiti. Oleh yang demikian, kami akan menyimpan data pelajar untuk tempoh yang lama bagi tujuan rekod. Bolehkah kami menyimpan data tersebut selama-lamanya? Ada keadaan di mana pelajar tahun 2002 mohon pengesahan kami mengenai status ijazah beliau bagi tujuan pekerjaan. Sekiranya rekod dan data beliau telah dihapuskan, sukar untuk kami memberi pengesahan tersebut.

Prinsip Penyimpanan APDP menetapkan bahawa data peribadi tidak boleh disimpan lebih lama dari tempoh ia diperlukan melainkan jika terdapat keperluan oleh peruntukan undang-undang yang lain. Tempoh penyimpanan yang melebihi keperluan tanpa peruntukan undang-undang lain memerlukan justifikasi yang kukuh dan perlu diperincikan di dalam Tataamalan Golongan Pengguna Data yang berkaitan.

? Adakah penyimpanan data peribadi mempunyai tempoh sebelum ia dilupuskan? Jika ada, berapa tahun?

Data peribadi yang diproses bagi apa-apa maksud tidak boleh disimpan lebih lama daripada tempoh yang diperlukan bagi memenuhi maksud tersebut.



? If a customer (purchaser) request for information kept by the company, does the company verify if the customer request for specific information or does the company just show the files kept by the company or the data kept in the computer?

It is up to the company to decide on the amount of disclosure of the requested data. However, do take note that a request for access by customer is only for the data requested.

What to do after a company has registered under the PDPA?

Once a company has registered as a Data User under the PDPA, the company may start to comply with the provisions of the Act.

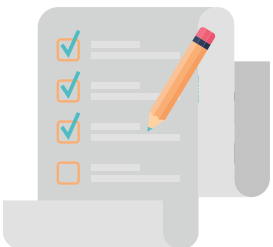
If the organization or company has been registered and there are two colleges under the company, is this registration applicable to both colleges?

In a situation where both colleges hold the same brand under one license by the Ministry of Education; the principal college will need to register and apply for CTC from the PDP Commissioner for all of its branches in Malaysia. However, if both colleges hold a separate license; then registration is applicable to both.

Should it be granted if Immigration request for company's EPF data?

As Immigration is a federal department, it is not bound to the PDPA. Additionally, pursuant to Section 39; the disclosure of personal data to authority can be granted such as for the prevention and detection of crime, and for investigation purposes. However, a data user should have a procedure in place to verify the authenticity of the request.

Do we need to delete guest's personal data if the guest has checked out?



Data users are not to retain personal data longer than necessary unless there are other legal provisions which requires longer retention of the data.

Is work contract bound by the PDPA?

Yes.

If we have branches around Sarawak, do we need to copy and display the certificate of registration at our branches? Will a copy in black and white do? Or do we need to get a copy from the Commissioner's Office?

Yes, under P.U.(A) 337/2013, Regulation 8(1) and Regulation 9; every branch needs to display a certified true copy of the registration certificate. The certified true copy can be applied via online at https://daftar.pdp.gov.my

Any compound for late renewal?

Late renewal of registration is regarded as processing personal data without a certificate of registration. It is an offence under Section 16(4) of the PDPA.

What is the significant difference for registered data user since compliance is mandatory?

The registered data user will be involved in a Data User Forum. The Forum is a platform for the establishment of a Code of Practice.

PENDAFTARAN
REGISTRATION

My company had registered in 2013. Currently our company is under renovation for at least 12 to 18 months. Do we need to renew our registration or just suspend the account until it resumes?

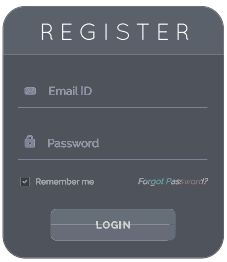
Registration is required for data users listed in the Class of Data Users under P.U.(A). 336/2013 and P.U.(A). 326/2016 that processes personal data for commercial transactions.

Apakah kriteria yang diperlukan untuk mendaftar syarikat di bawah APDP?

Pengguna data yang dinyatakan di dalam P.U.(A). 336/2013 atau P.U.(A). 326/2016.

Apa perbezaan yang diperolehi apabila mendaftar syarikat dibawah PDPA dan sekiranya tidak berdaftar?

Pengguna data yang berdaftar akan dikeluarkan Perakuan Pendaftaran dan akan ditubuhkan suatu Forum Pengguna Data. Forum Pengguna Data akan menyediakan suatu Tataamalan di mana ia dapat meningkatkan kepercayaan dan integriti dalam mengendalikan data peribadi.



Untuk PBT siapa yang perlu membuat pendaftaran?

Hanya pengguna data yang tersenarai di bawah P.U.(A) 336/2013 dan P.U.(A) 326/2016 yang diwajibkan pendaftaran di bawah APDP.

Kewajipan untuk melakukan pendaftaran bagi PBT?

Hanya pengguna data yang tersenarai di bawah P.U.(A) 336/2013 dan P.U.(A) 326/2016 yang diwajibkan pendaftaran di bawah APDP.

Adakah sesebuah syarikat Sdn. Bhd. yang memperuntukkan perkhidmatan akaun perlu didaftar? (Walaupun pengarah-pengarah bukan ahli MIA- *Malaysian Institute of Accountant*)

Tidak semestinya kerana hanya firma perakaunan yang berdaftar dengan pihak MIA yang perlu berdaftar dengan APDP.

Perlukah syarikat kejuruteraan yang menghasilkan alatan kilang untuk dijual kepada kilang pembuatan berdaftar di bawah APDP?

Pendaftaran adalah diwajibkan bagi Golongan Pengguna Data di bawah P.U.(A) 336/2013 dan syarikat tersebut mempunyai lesen oleh Lembaga Jurutera Malaysia.

How often does an employer need to organize awareness programme/training? Is it mandatory for every staff to attend the training/awareness programme? Will the PDP Office request for evidence that the individual attended the training?

The frequency of organizing awareness programme/training for staff will depend on the policy of a company. Awareness programme/training is one of the requirements under the PDP Standard. Yes, the Commissioner's Office will request for related evidence with regard to awareness programme/training held by the organization.

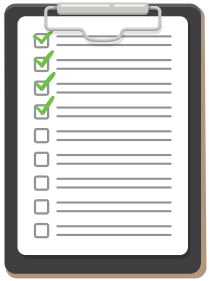
PDPA Standard: Do we need to have a book to register staff who has access to personal data. Can we use system to keep track?

Yes, you can.

What will be the area checked during your monitoring visits?

Monitoring visits will be focusing on the compliance of the 7 Principles of PDP.

? Dalam sesi standard ada menyebut tentang keperluan surat lantikan kepada kakitangan yang menggunakan data. Mohon pencerahan lebih lanjut mengenai hal ini. Jika tanggungjawab kakitangan untuk mematuhi APDP sudah dimasukkan dalam JD (Job Description) kakitangan, masih perlukah untuk mengeluarkan surat lantikan / kebenaran?



Bagi memenuhi Standard Keselamatan, kakitangan yang dikenalpasti untuk menguruskan data peribadi hanya perlu didaftarkan ke dalam sistem/buku pendaftaran sebelum dibenarkan mengakses data peribadi.

? Apakah persamaan yang diguna pakai dalam standard Akta 709 dengan standard ISMS (MS ISO 27001:2013)?

Standard Perlindungan Data Peribadi (Standard PDP) adalah standard yang telah dibangunkan berdasarkan ISO/IEC 27001:2013 Information Technology --Security Technique--Information Security Managemet System-Requirements (The ISMS). Standard PDP ini merangkumi tiga standard bagi Prinsip Keselamatan, Prinsip Penyimpanan dan Prinsip Integriti Data. Standard PDP merupakan keperluan minimun yang boleh dicapai bagi pematuhan APDP oleh pengguna data di Malaysia. Namun demikian, pengguna data yang telah memperolehi pensijilan ISMS ini adalah digalakkan untuk terus mengamalkannya dalam pemprosesan data peribadi.

? Apakah maklumat-maklumat penting yang diperlukan oleh pihak tuan sebelum subjek data membuat aduan masalah mengenai insurans? Contoh : nama insurans dan ?

Maklumat-maklumat yang diperlukan terhadap insurans adalah : Nama syarikat, alamat, nombor telefon yang boleh dihubungi, e-mel, isu yang diadukan dan dokumen sokongan(jika perlu).

? Mengenai pengguna data yang disiasat oleh Pesuruhjaya (notis siasatan dikeluarkan), adakah peguam pengguna data berurusan dengan Pejabat Pesuruhjaya bagi pihak anak guam? Atau wakil pengguna data sahaja yang berhak berurusan dengan Pejabat Pesuruhjaya? Bolehkah peguam berurusan dengan Pejabat Pesuruhjaya tanpa berjumpa dengan wakil pengguna data?

? Syarikat tersebut tidak memperoses apa-apa data untuk sendiri tetapi mengikut mandat yang diberikan oleh pelanggan. Adakah mana-mana seksyen APDP yang berkenaan dengan pengguna data kena dipatuhi oleh syarikat pemprosesan data tersebut?

? Adalah difahamkan (dari APDP) bahawa cuma seksyen-seksyen yang berkaitan dengan pemprosesan data yang kena dipatuhi jika pemproses tidak memproses apa-apa data yang diterima demi pelanggan untuk faedah pihak pemproses data sendiri.

Pengguna data atau peguam yang dilantik boleh berurusan dengan Pejabat Pesuruhjaya.

Setiap pengguna data yang memproses data pelanggannya perlu patuh kepada 7 Prinsip PDP, Standard PDP dan Tataamalan. Pemproses data yang bertindak bagi pihak pengguna data juga perlu mematuhi perkara-perkara tersebut. Walau bagaimanapun, jika berlaku pelanggaran terhadap APDP oleh pemproses data, pengguna data akan bertanggungjawab di atas pelanggaran tersebut.

How are insurance agents / third party be held responsible for the breach of the PDPA?

The requirements of the PDPA must be stated in contracts and its compliance be communicated clearly with the insurance agents/third party. With that, any breach on their part will position the responsibility for the breach to the insurance agents/third party.

Does the Act apply to the *social media* like Facebook/ Wechat etc., which doing the online business. Example: Some details need to be provided to the seller on Facebook when we purchase costume online.

The Act applies to any personal data processed for commercial transactions.

Bagaimanakah dengan data individu yang digunakan sebagai data perniagaan. Contoh milikan tunggal dan pengkongsian, perlukah dimusnahkan jika diminta oleh subjek data sedangkan data adalah data perniagaan

Bagi data individu yang digunakan sebagai data perniagaan, rujukan perlu dilakukan terlebih dahulu kepada Akta ibu, contohnya Akta Syarikat 2016.

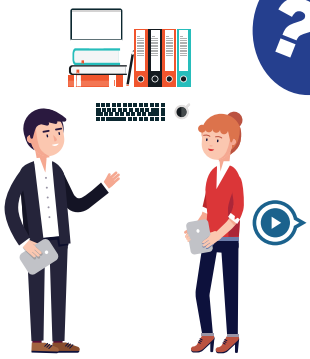
Adakah Jabatan Kerajaan, Kerajaan Tempatan dan Badan Berkanun terlibat dengan pemakaian PDPA dan denda yang dikenakan juga terpakai kepada badan-badan di atas?

Kerajaan Tempatan dan Badan Berkanun turut dituntut pematuhan terhadap APDP dan denda yang dikenakan di bawah APDP juga terpakai kepada badan-badan tersebut.

LAIN-LAIN
OTHERS

Seringkali yang datang ke kaunter adalah pihak ketiga dan bukan pemilik sendiri. Adakah sah perakuan yang ditandatangani oleh wakil bagi pihak pemilik?

Keadaan ini akan tertakluk kepada prosedur operasi standard (SOP) pengguna data.



Siapakah yang akan dikenakan pertuduhan jika terdapat kejadian kebocoran maklumat data peribadi pengguna syarikat dan pekerja?

Di bawah Seksyen 133(1) APDP, mana-mana orang yang pada masa pelakuan kesalahan itu ialah seorang pengarah, ketua pegawai eksekutif, ketua pegawai operasi, pengurus, setiausaha atau pegawai lain yang bertanggungjawab semasa berlakunya kesalahan boleh dipertuduh secara berasingan atau bersesama dalam prosiding yang sama bersekali dengan pertubuhan perbadanan itu.

Jika ada perkara negatif keluar di Facebook dan telah dilaporkan kepada pihak polis, adakah kes tersebut di bawah bidang kuasa KKMM?

Kes tersebut adalah di bawah bidang kuasa SKMM dan akan akan disiasat di bawah Akta berkaitan.

Bagaimana nak tahu data peribadi sensitif? Apakah standard yang diguna pakai?

Di bawah APDP, "data peribadi sensitif" merupakan apa-apa data peribadi yang mengandungi maklumat tentang kesihatan atau keadaan fizikal atau mental seorang subjek data, pendapat politiknya, kepercayaan agamanya atau kepercayaan lain yang bersifat seumpamanya, perlakuan atau pengataan pelakuan apa-apa kesalahan olehnya atau apa-apa data peribadi lain yang ditentukan oleh Menteri melalui perintah yang disiarkan dalam Warta.

First Print, 2017
All rights reserved.

Any part of this publication may not be reproduced, stored in, or transmitted in a permanent storage system, or transmitted in any form or by any means,electronically, mechanically, photocopying, recording or otherwise without the prior consent of the Personal Data Protection Commissioner Malaysia.

PESURUHJAYA PERLINDUNGAN DATA PERIBADI MALAYSIA
The Personal Data Protection Commissioner Malaysia

Aras 6, Kompleks Komunikasi Dan Multimedia Malaysia,
Lot 4G9, Presint 4, Persiaran Perdana,
Pusat Pentadbiran Kerajaan Persekutuan, 62100 Putrajaya

w w w . p d p . g o v . m y

03 89115000
03 8000 8000 (1MOCC)

aduan@pdp.gov.my

03 8911 7959

www.pdp.gov.my