

# THE PRINCIPLES OF PERSONAL DATA PROTECTION UNDER THE MALAYSIAN PDPA 2010

TALK FOR THE FACULTY OF MANAGEMENT  
MULTIMEDIA UNIVERSITY, CYBERJAYA  
9 September 2021

ASSOC. PROF. DR. SONNY ZULHUDA  
International Islamic University Malaysia



[sonny@iium.edu.my](mailto:sonny@iium.edu.my)



[sonnyzulhuda.com](http://sonnyzulhuda.com)



[twitter.com/zulhuda](https://twitter.com/zulhuda)



**LEADING THE WAY**  
KHALIFAH · AMĀNAH · IQRA' · RAHMATAN LIL-ĀLAMĪN



AN INTERNATIONAL AWARD-WINNING INSTITUTION FOR SUSTAINABILITY

# Agenda Today

## 01 Introduction

What & Why Privacy? | Reality Check | About Personal Data Protection Act | Case Studies & Data Breach Cases

## 02 Data Protection Principles

Understanding the Key Principles | Internalising the Best Practices | Offences upon Breach

## 03 Discussion



1

# INTRODUCTION



# What is Privacy?



Right to Life, to Enjoy Life with Dignity 

"Leave me Alone" – Right to Solitude 

Right to be Anonymous, under no Scrutiny 

Informational Privacy: Identity, Communications, lifestyle, etc 

**84%**

of respondents indicated that they care about privacy, care for their own data, care about the data of other members of society, and they want more control over how their data is being used.

[Cisco Consumer Privacy Survey 2019](#)

# Data Privacy at Stake



## Switching Providers

48% indicated they already switched companies or providers because of their data policies or data sharing practices. **Cisco Consumer Privacy Survey 2019**

48%



## Concerned about Companies

79% of respondents said they are very or somewhat concerned about how companies are using the data they collect about them. **Pew Research Center**

79%



## Concerned about Gov

64% say they have the same level of concern about government data collection. **Pew Research Center**

64%



## Losing Control

81% of respondents feel as if they have little or no control over the data collected. **Pew Research Center**

81%



## DIGITAL ECONOMY

Emergence of five key drivers for the digital economy, namely (1) Datafication; (2) Social Media; (3) IoT; (4) Machine learning; (5) Synchronisation

## WHO MISUSE YOUR DATA?

Three BIGS around us: (1) BIG Brother; (2) BIG Data Aggregator; (3) BIG Fans, for good or less-good reasons.



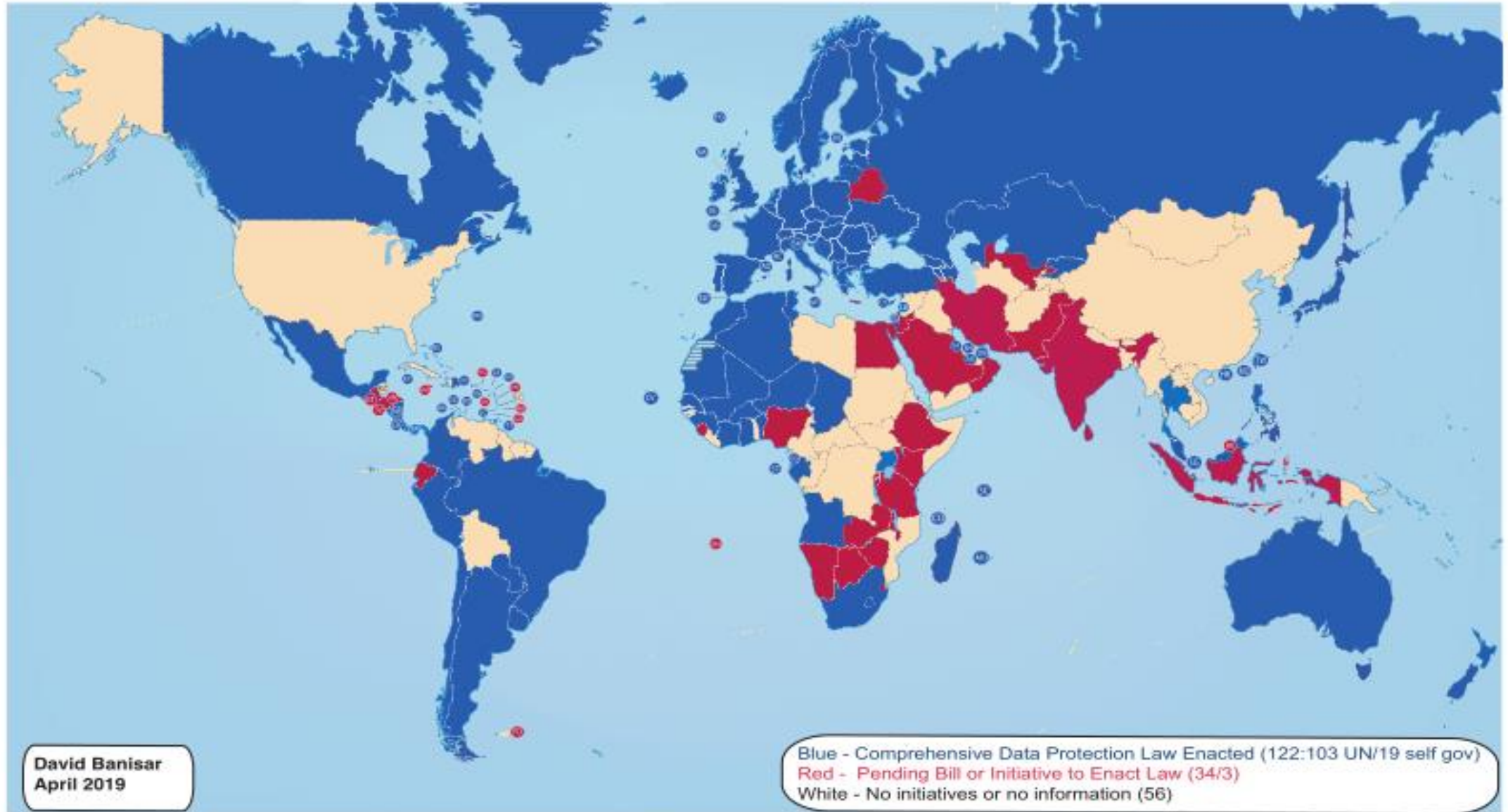
## RISKS OF PERSONAL DATA BREACHES

With (1) Increasing reliance to cyber system and data analytics in both private and public infrastructure; (2) Abundant data in public domain; (3) Increasing non-state actors in data breaches and cyber terrorism.

**DATA BREACH IS A MATTER OF WHEN, NOT IF!**



# National Comprehensive Data Protection/Privacy Laws and Bills 2019



# PDPA 2010 (Act 709)

An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.



Malaysia is the first country in ASEAN to have enacted data privacy law, followed by Singapore (2012), Philippines (2012), and Thailand (2019).

**PERSONAL DATA:** Those that relates directly or indirectly to a data subject, who is identified or identifiable from that information (or from that and other info in the possession of a data user)



Applies to “Data Users” and “Data Processors” in respect of **commercial transactions**.



Must be established in Malaysia; or not – as long as he uses equipment in Malaysia for data processing. Eg. Cloud Service, or BPO in Malaysia.



Not applicable to the “Federal Govt and State Govts”.

See: Muniandy A/L Subramaniam & Ors v Majlis Perbandaran Langkawi & Anor [2003] 6 MLJ 177

# Rights of Data Subjects

(Hak-hak Subjek Data)

An infographic titled "HAK-HAK SUBJEK DATA" (Rights of Data Subjects) from the Malaysian Personal Data Protection Department (PDPA). The infographic features a central graphic of a blue diamond with a fingerprint-like pattern. It lists five rights: 1. HAK UNTUK MENGHALANG PEMROSESAN BAGI MAKSUD PEMASARAN LANGSUNG (Right to object to direct marketing processing); 2. HAK UNTUK MENGAKSES (Right of access); 3. HAK UNTUK MEMBUAT PEMBETULAN (Right to correction); 4. HAK UNTUK MENARIK BALIK PERSETUJUAN (Right to withdraw consent); 5. HAK UNTUK MENGHALANG PEMROSESAN YANG MUNGKIN MENYEBABKAN KEROSAKAN ATAU DISTRES (Right to object to processing that may cause damage or distress). The infographic includes the PDPA logo, the hashtag #jomambilpeduli, the hashtag #lindungidataperibadi, and the website www.pdp.gov.my.

**JABATAN PERLINDUNGAN DATA PERIBADI**

## HAK-HAK SUBJEK DATA

- 1 HAK UNTUK MENGHALANG PEMROSESAN BAGI MAKSUD PEMASARAN LANGSUNG**
- 2 HAK UNTUK MENGAKSES**
- 3 HAK UNTUK MEMBUAT PEMBETULAN**
- 4 HAK UNTUK MENARIK BALIK PERSETUJUAN**
- 5 HAK UNTUK MENGHALANG PEMROSESAN YANG MUNGKIN MENYEBABKAN KEROSAKAN ATAU DISTRES**

#jomambilpeduli  
#lindungidataperibadi

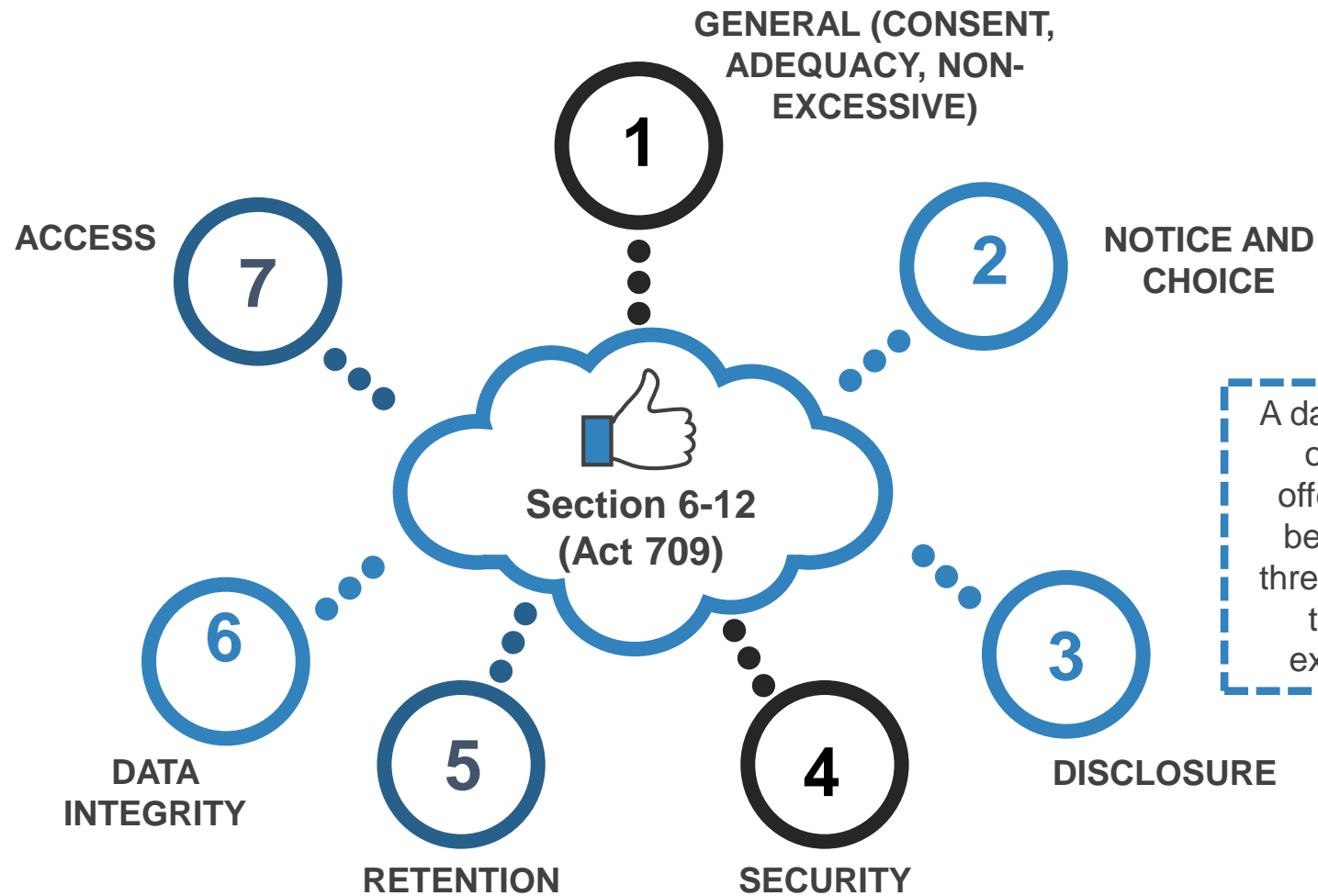
[www.pdp.gov.my](http://www.pdp.gov.my)

2

# DATA PROTECTION PRINCIPLES



# Seven Data Protection Principles



A data user who contravenes any of these principles commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.



# General Principle



- Data user shall not process personal data about a data subject unless the data subject has given his **consent** to the processing of the personal data (section 6 PDPA)

## Personal data shall not be processed unless

1. the personal data is processed for a **lawful purpose** directly related to an activity of the data user;
2. the processing of the personal data is **necessary** for or **directly related** to that purpose; and
3. the personal data is **adequate but not excessive** in relation to that purpose.

# Notice and Choice Principle

When first collecting or acquiring the personal data, Data User shall inform the Data Subject in a written notice about:

- Nature of the personal data being collected and processed
- Purpose of processing
- Source of data
- Rights of access, correction and manners of inquiries or complaint
- Third parties to whom data will be disclosed
- Choice and means to limit the processing
- Whether supply of personal data is obligatory or voluntary; and what would be the consequences of failure if it is obligatory.

The data users must also notify data subjects on how to contact the data users with any inquiries or complaints in respect of the personal data.



# Disclosure Principle

No personal data shall, without the consent of the data subject, be disclosed:

- a) for any purpose not originally notified when the data was first collected, or not directly related to that original purpose
- b) to any third party not initially notified when the data was first collected.



# Security Principle



Data user shall take **practical steps** to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction

Cross-refer: Security Standard under PDP Regulations 2013

**“Practical steps” means both technical and organizational measures**

The steps should take into account:



NATURE OF  
HARM



LOCATION OF  
STORAGE



SECURITY OF  
EQUIPMENT



COMPETENCE  
OF PERSONNEL



MEASURES OF  
TRANSFER

# Retention Principle

The personal data shall not be kept longer than is necessary for the fulfillment of its purpose.

- How long? Question of fact. Not fixed under PDPA 2010
- How to dispose the data?
- Best Practice: **Data Anonymisation!**



# Data Integrity Principle

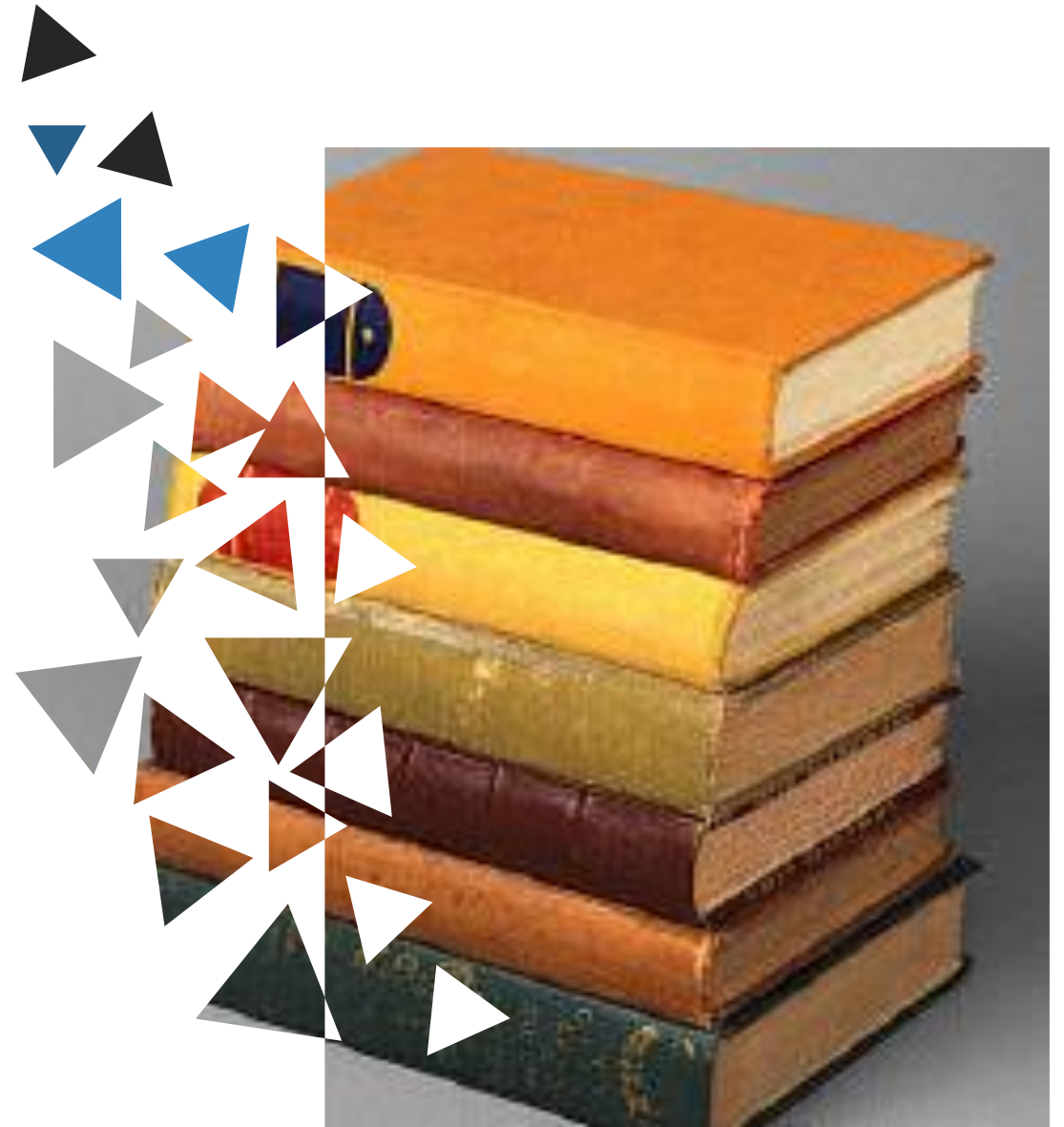
Data user shall take reasonable steps...

to ensure that the personal data is accurate, complete, not misleading and kept up-to-date



# Access Principle

Data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date



# New Offences under PDPA

Breaching data protection principles

Failure to register as Data User (when applicable)

Unlawful collection of personal data

Unlawful sale of personal data

Breach of data security system

# Data Privacy Today

## Universiti Malaya, JPDP looking into report of massive data breach affecting the university

TECH

Saturday, 19 Oct 2019

1:34 PM MYT

By Qishin Tariq



HOME / MALAYSIA

## Deputy minister: Probe to determine if 2018's massive telco data leak due to sabotage or hacking

Tuesday, 26 Nov 2019 11:44 PM MYT

## Malindo Air says data breach caused by ex-employee of e-commerce firm

Justin Lim / [theedgemarkets.com](http://theedgemarkets.com)

September 23, 2019 16:13 pm +08

## UiTM students' data allegedly stolen

NATION

Saturday, 26 Jan 2019

12:00 AM MYT

PETALING JAYA: Private information of over a million student Teknologi MARA (UiTM) enrolled between 2000 and 2018 has been exposed in a data breach.

## Hacker claims to have stolen personal data of Universiti Malaysia Sabah students

TECH

Tuesday, 05 Nov 2019

4:50 PM MYT

By Angelin Yeoh



## Over 17,000 patients' personal data exposed on national neurology registry website

NATION

Wednesday, 23 Oct 2019

12:12 PM MYT

PETALING JAYA: In yet another data breach, more than 17,000 patients' personal data have been exposed on the government-linked National Neurology Registry (NNeuR) website due to a scripting error, news portal Free Malaysia Today (FMT) reported.

# Taking patient's picture without consent breaches privacy - Lee Ewe Poh v Dr Lim Teik Man [2011] – High Court Penang



**PENANG:** Privacy breach is actionable. Court said that the privacy right of a female in relation to her **modesty, decency and dignity** in the context of the high moral value is her fundamental right.

# Data Leakage due to Exiting employees

Equity Trust (Labuan) Ltd v Mohammad Sofian Mohamad [2010] – Labuan



**LABUAN:** Court issued injunction to stop a former employee marketing staff from disclosing confidential information including **clients' listing and potential clients data** to a new employer (2010)

# Offences by Body Corporate

## Sec 133 – What is it?

When an offence is committed by a data user as a body corporate (i.e in his capacity as the staff there)

## What will happen next?

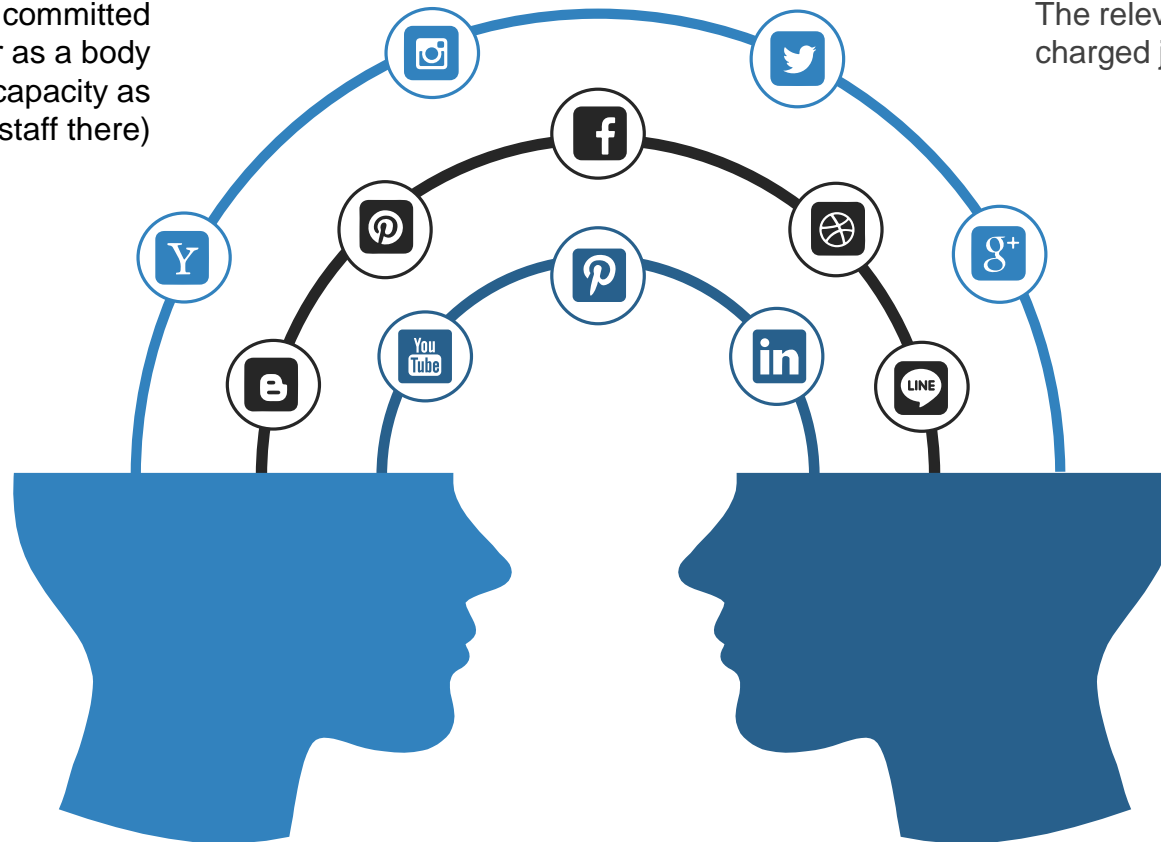
The relevant officers may be charged jointly or severally,

## What will happen?

That corporation being the data user will be held liable and subject to punishment.

## What defense is available?

when the officer can prove:  
Absence of his knowledge, AND  
Exercise of due diligence





## SIARAN MEDIA

### PENYALAHGUNAAN DATA PERIBADI OLEH APLIKASI DALAM TALIAN PEMBERI PINJAM WANG TIDAK BERLESEN

**PUTRAJAYA, 20 NOVEMBER 2020 (JUMAAT)** – Merujuk kepada siaran media Jabatan Perlindungan Data Peribadi (JPDP) bertarikh 5 Oktober 2020, JPDP masih lagi menerima banyak aduan berkaitan dengan penyalahgunaan data peribadi oleh aplikasi dalam talian Pemberi Pinjam Wang (PPW) tidak berlesen.

Dalam hal ini JPDP, dengan kerjasama CyberSecurity Malaysia dan Suruhanjaya Komunikasi dan Multimedia Media (SKMM), telah membuka Kertas Siasatan bagi pelanggaran di bawah seksyen 5 Akta Perlindungan Data Peribadi 2010 [Akta 709] ke atas aplikasi dalam talian PPW tidak berlesen seperti berikut:

- (a) Asialend;
- (b) Dreamlend;
- (c) iPayfren;
- (d) iPinjaman;
- (e) Helpend4u; dan
- (f) GoCash4u.

Sekiranya disabitkan, entiti berkenaan boleh didenda tidak melebihi RM300,000.00 atau dipenjarakan selama tempoh tidak melebihi dua (2) tahun atau kedua-duanya sekali.

Kesemua aplikasi dalam talian PPW ini didapati telah mengakses dan menyalin maklumat lain termasuk data peribadi yang tidak berkaitan dengan urusan pinjaman tanpa kebenaran peminjam.

Sehubungan dengan itu, mana-mana peminjam yang data peribadinya telah disalahgunakan oleh aplikasi dalam talian PPW tidak berlesen tersebut di atas, diseru untuk menghubungi Bahagian Penguatkuasaan JPDP melalui alamat e-mel [penguatkuasaan@pdp.gov.my](mailto:penguatkuasaan@pdp.gov.my) atau Sistem Perlindungan Data Peribadi ([daftar.pdp.gov.my](http://daftar.pdp.gov.my)) bagi membantu siasatan yang dijalankan.

JPDP amat memandang serius mengenai perkara ini dan mengesyorkan supaya rakyat Malaysia agar lebih berhati-hati apabila membuat sebarang pinjaman secara dalam talian terutamanya semasa memberikan persetujuan terhadap aplikasi yang





## SIARAN MEDIA

### INSIDEN KETIRISAN DATA PERIBADI YANG MELIBATKAN PELANGGAN SHOPBACK CASHBACK SDN. BHD. ("SHOPBACK")

PUTRAJAYA, 27 SEPTEMBER 2020 (AHAD) - Jabatan Perlindungan Data Peribadi (JPDP) telah menerima notifikasi ketirisan data peribadi melalui wakil yang telah dilantik oleh ShopBack Cashback Sdn. Bhd. ("ShopBack") pada 25 September 2020 (Jumaat) jam 06:01 petang susulan daripada penemuan ketirisan data peribadi yang melibatkan data peribadi pelanggan ShopBack pada 17 September 2020 seperti nama, maklumat perhubungan, jantina, tarikh lahir dan nombor akaun bank.

Notifikasi tersebut telah memaklumkan bahawa ShopBack akan mula menghubungi para pelanggannya melalui alamat e-mel yang telah didaftarkan selain penyediaan laman khusus soal jawab (Q&A) dalam memberi pencerahan serta langkah-langkah selanjutnya yang boleh diambil. Selain itu, Jabatan ini telah dimaklumkan berhubung langkah-langkah mitigasi yang telah diambil oleh ShopBack sehingga kini dalam menangani insiden berkenaan. ShopBack juga telah memberi jaminan bahawa semua langkah mitigasi yang telah diambil akan dapat mengekang sepenuhnya insiden ketirisan data peribadi ini daripada berlanjutan.

Pada masa yang sama, Jabatan ini akan mendapatkan maklum balas lanjut daripada ShopBack termasuklah jumlah sebenar data peribadi rakyat Malaysia yang terlibat. Jabatan ini juga akan bekerjasama rapat dengan semua pihak yang berkepentingan dalam menilai tahap keparahan (*severity*) insiden ketirisan data peribadi ini selaras dengan peruntukan di bawah Akta Perlindungan Data Peribadi 2010 [Akta 709].

Jabatan ini amat memandang serius perkara ini dan ingin menyeru semua Pengguna Data di Malaysia agar sentiasa memastikan keselamatan data peribadi Subjek Data di bawah kendalian masing-masing seperti yang telah termaktub di bawah Akta 709 untuk dilindungi sepenuhnya.

JABATAN PERLINDUNGAN DATA PERIBADI

Untuk maklumat lanjut mengenai siaran media ini, sila hubungi UKK JPDP di talian +603-89117911



## SIARAN MEDIA

### ADUAN PENYALAHGUNAAN DATA PERIBADI OLEH SYARIKAT ASIALEND (MY) SDN. BHD. ("ASIALEND")

PUTRAJAYA, 5 OKTOBER 2020 (ISNIN) – Jabatan Perlindungan Data Peribadi (JPDP) telah menerima banyak aduan berhubung penyalahgunaan data peribadi yang telah dikumpulkan secara tidak sah oleh Syarikat Asialend (MY) Sdn. Bhd ("Asialend"). Asialend adalah merupakan sebuah syarikat Pemberi Pinjam Wang (PPW) yang tidak berdaftar melalui semakan dengan Kementerian Perumahan dan Kerajaan Tempatan (KPKT).

Pihak Asialend juga didapati telah menyalahgunakan maklumat syarikat Cashwagon (M) Sdn. Bhd. dan notis tersebut boleh dicapai seperti di pautan berikut, <https://cashwagon.my/blog/important-notice-scanv/>.

Dalam hubungan yang sama, rakyat Malaysia dimohon untuk lebih berhati-hati semasa memberikan persetujuan terhadap aplikasi yang telah dimuat turun bagi mengelakkan pihak-pihak yang tidak bertanggungjawab mempunyai akses yang tidak sepatutnya.

Bagi sebarang aduan penyalahgunaan data peribadi oleh Asialend atau syarikat PPW yang lain, semua pihak dialu-alukan untuk melaporkan aduan berkenaan di pautan <https://daftar.pdp.gov.my> untuk tindakan Jabatan ini selanjutnya.

Jabatan Perlindungan Data Peribadi  
Kementerian Komunikasi dan Multimedia Malaysia

#JomAmbilPeduli  
#LindungiDataPeribadi

# Conclusion: New Norms brought by the PDPA 2010



A

Affirm the  
Privacy  
Expectation for  
Malaysians

B

Business  
as Usual  
No More

C

Culture of  
Respect,  
Transparency and  
Accountability

D

Defining New  
Rules, New  
Offences

# THANK YOU

## DR SONNY ZULHUDA

*Associate Professor at the International  
Islamic University Malaysia*



[sonny@iium.edu.my](mailto:sonny@iium.edu.my)



[sonnyzulhuda.com](http://sonnyzulhuda.com)



[twitter.com/zulhuda](https://twitter.com/zulhuda)

