Personal Data Protection Law in Malaysia

Mazmalek bin Mohamed
Director General
Personal Data Protection Department
Ministry of Communications & Multimedia
ACT 709

(PERSONAL DATA PROTECTION ACT 2010)
Siapakah yang memiliki data peribadi rakyat Malaysia?

Kerajaan?
(Akses secara sistematik)

Google? Facebook? Twitter?
LinkedIn? Enjin Carian lain?/
Groupon/Lazada?

Pemilikan secara konteks?
(Lain-Lain) – Bank/Telco/Insurans/Hotel/
Pemaju Perumahan/Peguam/Doktor/
Utiliti
World’s Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 1 April 2019

Filter Colour YEAR DATA SENSITIVITY

Latest
- Bitdefender
- BitInfo
- Bitdefender
- BitDefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitdefender
- Bitde
Malaysian data breach sees 46 million phone numbers leaked

By NST - January 27, 2019 @ 8:05am

IT has happened again. This time at Universiti Teknologi MARA (UiTM) where records of just over a million students have been leaked.

Is it an inside job? Hard to tell, but UiTM is probing.

UiTM sources contacted by The Star say it may just be put together from multiple sources by some hackers to make it look like it is from the university’s database.

The reason: screenshots of the leaked data scanned are not in the format used by UiTM. We have no reason to doubt this as the institution’s firewall has been strong. Plus, this is the university which has put a satellite – UiTM-SAT-1 – in orbit and is in the process of launching another, this time in collaboration with six others, by 2021.

So they do know a fair bit about firewall and data security.

If UiTM is right, the culprits must be out there, either in Malaysia or beyond. They are not unreachable, though a little difficult to identify.

The Malaysian Communications and Multimedia Commission (MCMC) must actively pursue them and bring them to book. We are still smarting from Malaysia’s biggest data breach in October 2017 when 46.2 million mobile subscribers’ data, among others, were leaked online.

Imagine the scale of the leak.

Malaysian population is only 29 million while the leaked data are just shy of 50 million.

We have the Personal Data Protection Act 2010 (PDPA) which regulates the processing of personal data in regard to commercial transactions but has it been enforced with vigour?

Not as vigorously as we expect given the number and scale of data breaches since PDPA was gazetted in June 2010.

The first data user – a local private college – was not charged until May 3, 2017 for processing personal data of former employees of the college without a valid certificate of registration in

Malaysia’s data breach sees 46 million phone numbers leaked

Sources:

Stolen data

The individual was trying to sell a huge amount of private customer information from at least 12 Malaysian mobile operators.

A massive data breach has seen the customer data of more than 46 million mobile subscribers in Malaysia leaked online to the dark web.


Sources:

Data Breaches Dent Singapore’s Image as a Tech Innovator

By Mike Ives
Jan. 30, 2019

HONG KONG — Singapore takes pride in being a technology hub where municipal decisions are driven by cutting-edge data science.

“Data is the new currency, and with open data, the possibilities are endless!” the government says on its “Smart Nation” portal.

But that image has been dented by two embarrassing data breaches.

Last year, a cyberattack on Singapore’s public health system compromised data from 1.5 million people. And on Monday, the Health Ministry said that medical records for 14,200 HIV-positive people in the city-state had been obtained by an American whose Singaporean partner worked at the ministry. The ministry said it learned on Jan. 22 that the records had been illegally disclosed online.

Experts say the breaches highlight the potential pitfalls for Singapore and other countries that are pushing to make vast troves of data more accessible and centralized. Do the public benefits justify the inherent risks to privacy? And can anyone prevent senior officials from

Sources:
WHY PROTECT PERSONAL DATA?

What Customers and International Organizations Say....

- Data protection is not just about protecting our personal information.
  Biometric data stored in one social-protection program database can easily be linked to other systems using a common identifier, even those unrelated to social protection, such as for law enforcement or commercial marketing. (World Economic Forum 2019)

- A global survey of 16,000 online customers across 20 countries found that 74% were concerned about how companies use information about them collected online. (United Nations Conference on Trade and Development (UNCTAD) 2016)

- Personal data is precious and priceless – protect it! (Internet Society 2016)

- Globally 40% of respondents said that they would never again do business with a company that suffered from data breach. (Global Commission on Internet Governance 2016)

- Users worldwide are not confident that their personal data are protected. Two in three users thought people who go on the Internet put their privacy at risk. (World Economic Forum 2013)
64% Believes managing people’s data is a corporate differentiating factor

84% Say breaches of data privacy and ethics causes them to lose trust in companies

90% Thinks that breaches of data privacy and ethics have negative impact on stakeholder trust levels in their industry in the next 5 years

From 1379 CEOs interviewed in 79 countries
PERSONAL DATA PROTECTION ACT 2010 (ACT 709)

01. One of the recognized cyber legislation in the implementation of the Multimedia Super Corridor

02. The 10th policy goal set out in CMA 1998 which is to ensure information security, and network reliability & integrity

03. Regulates the processing of personal data in commercial transactions

04. Applies to organizations that process personal data in commercial transactions e.g. Bank, Telco, Insurance, Hospital & etc.
IMPORTANCE OF THE ACT 709

To enhance public confidence and trust with ongoing enforcement.

To avoid and minimize the incidents of data breach.

To increase the efficiency and governance of personal data handling.

To ensure prudence and integrity in personal data handling.
### Data User
A person who either alone or jointly processes any personal data or has control over or authorizes the processing of any personal data.

![maxis]

### Data Processor
Any person, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.

E.g. Third parties/ vendors/ dealers.

![Logos of various companies]

### Data Subject
An individual who is the subject of the personal data. E.g. students, patients, employees, citizens, non-citizens, customers.
PROCESSING OF PERSONAL DATA

Collecting  Recording  Alteration

Holding  Storing  Transfer

Erasure  Correction  Retrieval

Destruction  Alignment  Combination
<table>
<thead>
<tr>
<th>Data Type</th>
<th>Personal Data</th>
<th>Sensitive Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Information</td>
<td>- Name</td>
<td>✓ Race, religion, health, political opinion, offence records</td>
</tr>
<tr>
<td></td>
<td>✓ IC numbers, passport numbers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓ Driver’s license, birth certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓ Bank account numbers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓ Home address, personal phone no.</td>
<td></td>
</tr>
<tr>
<td>Individual Customer Information</td>
<td>- Name</td>
<td>✓ Race, religion, health, political opinion, offence records</td>
</tr>
<tr>
<td></td>
<td>✓ IC numbers, passport numbers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓ Personal phone number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓ Home address, email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓ Bank account numbers</td>
<td></td>
</tr>
</tbody>
</table>

**WHAT IS PERSONAL DATA?**

Personal data includes information that can be used to identify an individual. Sensitive personal data includes information that can reveal someone’s identity or circumstances, such as race, religion, health, political opinion, or criminal records.
WHAT IS COMMERCIAL TRANSACTIONS?

SERVICES
INVESTMENT
TRADING
BANKING
INSURANCE

BUSINESS ACTIVITIES
NON-APPLICABILITY PDPA 2010

Federal & States Government

Personal, Family, Household Affairs

Data Processed Outside of Malaysia

Non-Commercial Transactions

Credit Reporting Agencies
Class of Data Users

COMMUNICATIONS
- Licensee under the Communications and Multimedia Act 1998
- Licensee under the Postal Services Act 2012

BANKING AND FINANCIAL INSTITUTION
- Investment bank under the Financial Services Act 2013
- Islamic bank under the Islamic Financial Services Act 2013
- Development Financial Institution under the Development Financial Institution Act 2002

INSURANCE
- Insurer under the Financial Services Act 2013
- Takaful operator under the Islamic Financial Services Act 2013
**HEALTH**
- Hospital or clinic under the Private Healthcare Facilities and Services Act 1998
- Body corporate under the Registration of Pharmacists Act 1951

**TOURISM AND HOSPITALITIES**
- Travel agent or Hotel under the Tourism Industry Act 1992

**TRANSPORTATION**
- MAB, Air Asia, MAS Wings, Air Asia X, Firefly, Berjaya Air, or Malindo Air

**EDUCATION**
- Priv. higher edu. inst. under the Private Higher Educational Institutions Act 1996
- Priv. school or educational institution registered under the Education Act 1996
DIRECT SELLING
• Licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993

SERVICES
• Legal, audit, accountancy, engineering or architecture firm
• Retail dealing and wholesale dealing as defined under the Control Supplies Act 1961
• Private employment agency under the Private Employment Agencies Act 1981

REAL ESTATE
• Housing developer under the Housing Development (Control and Licensing) Act 1966
• Housing Development (Control and Licensing) Enactment 1978, Sabah
• Housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak
UTILITY
• Electricity and Water

PAWNBROKER
• Licensee under the Pawnbrokers Act 1972

MONEYLENDER
• Licensee under the Moneylenders Act 1951
Exemptions

Partial

Prevention / Detection Crime
Statistics / Research
Tax / Duty Assessment / Collection
Regulatory Functions
Court Order / Judgment
Offenders Apprehension / Prosecution
Physical / Mental Health
Journalistic / Literary / Artistic
# The Principles of Data Protection

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>01</strong> GENERAL</td>
<td>Personal data shall be adequate, relevant and not excessive. Processed with consent and for a lawful purpose</td>
</tr>
<tr>
<td><strong>02</strong> NOTICE &amp; CHOICE</td>
<td>Inform the purposes for which the personal data is being processed, collected or disclosed</td>
</tr>
<tr>
<td><strong>03</strong> DISCLOSURE</td>
<td>Disclosure without consent is not permissible</td>
</tr>
<tr>
<td><strong>04</strong> SECURITY</td>
<td>Protect data from loss, misuse, unauthorized access, etc.</td>
</tr>
<tr>
<td><strong>05</strong> RETENTION</td>
<td>Personal data shall not be kept longer than necessary</td>
</tr>
<tr>
<td></td>
<td>• How much to retain data?</td>
</tr>
<tr>
<td></td>
<td>• How long does it take?</td>
</tr>
<tr>
<td></td>
<td>• How to store data?</td>
</tr>
<tr>
<td><strong>06</strong> DATA INTEGRITY</td>
<td>Personal data shall be accurate, up-to-date, verifiable</td>
</tr>
<tr>
<td><strong>07</strong> ACCESS</td>
<td>The right to access personal data.</td>
</tr>
</tbody>
</table>
The Personal Data Protection Standard is a minimum requirement issued by the Commissioner, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results.

This standard applies to:
Any person who processes; and
Any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions.

It’s a minimum standard which comprises of three personal data protection principles, namely security, retention and data integrity.
PERSONAL DATA PROTECTION STANDARD
(Electronically and non-Electronically)

**Security Standard**
- Update the Back up / Recovery System & anti-virus to prevent personal data intrusion
- Control and limit employees’ access to personal data system
- Record personal data transferred conventionally such as through mail, delivery, fax, and etc.

**Retention Standard**
- Keep personal data no longer than necessary unless there are requirements by other legal provisions
- Determine the retention period in all legislation before destroying personal data e.g.: s.82 Income Tax Act 1967 (7 years)

**Data Integrity Standard**
- Notify on personal data updates by appropriate methods
- Provide personal data update form for data subjects
- Update personal data immediately
HOW THE PDPA 2010 IMPROVES THE DATA GOVERNANCE

1. Spells out the duties throughout data lifecycle
2. Sets up data management standard
3. Identifies data risks
4. Improves security measures
5. Promotes data integrity
1. Create awareness in the organisation
   1. Awareness of internal policies for securing personal data
   2. To inculcate the culture of personal data protection

✓ Knowing your current compliance level
   • Understand the impact of PDPA 2010
   • Identify the gaps

✓ Designate a Data Protection Officer or Committee
   • Define a data protection strategy
   • Develop a short term compliance programme

✓ Develop polices for PDPA 2010
   • Policies spanning across legal, IT, marketing, human resource, customer services, etc.
   • Focus on end-to-end data governance processes, policies and procedures in line with the PDPA 2010.
Rights of Data Subjects

1. Right to Prevent Processing for Direct Marketing
2. Right to Prevent Processing Likely to Cause Distress
3. Right to Withdraw Consent
4. Right to Make Correction
5. Right to Access
Elements Notification

A. DETAILS ABOUT THE DATA BREACH
   • Summary of the event and circumstances.

B. CONTAINMENT OR CONTROL MEASURES
   • Details of actions / measures taken or will be taken to contain the breach.

C. NOTIFICATION
   • Who has been notified about the breach?

D. TRAINING AND GUIDANCE IN RELATION TO DATA PROTECTION
   • Does the organization provide training / awareness programme to staff?
Data and Digital Economy
“Data is the new Oil”

– Clive Humby
If data is the new oil

Understand your
- strategy
- organizational impact
- data landscape

before selecting your drill
Any individual or relevant person may make a complaint in writing to the Personal Data Protection Commissioner:

- via online system daftar.pdp.gov.my; or

Address to:

Personal Data Protection Commissioner
Level 6, Kompleks KKMM,
Lot 4G9, Persiaran Perdana,
Presint 4, 62100
Putrajaya.
Thank You