DATA PRIVACY

Objectives

- To describe key elements of the Personal Data Protection Act 2012 (PDPA)
- To understand data protection obligations prescribed by PDPA
- To understand the impact of the EU GDPR

Agenda

- **What is Data Privacy**
- What is Personal Data
- Data Protection Obligations
- GDPR Highlights

The Guardian

I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets

The dating app knows me better than I do, but these reams of intimate information are just the tip of the iceberg. What if my data is hacked – or sold?

Tue 26 Sep 2017 07.10 BST

At 9.24pm (and one second) on the night of Wednesday 18 December 2013, from the second arrondissement of Paris, I wrote “Hello!” to my first ever Tinder match. Since that day I’ve fired up the app 920 times and matched with 870 different people. I recall a few of them very well: the ones who either became lovers, friends or terrible first dates. I’ve forgotten all the others. But Tinder has not.

The dating app has 800 pages of information on me, and probably on you too if you are also one of its 50 million users. In March I asked Tinder to grant me access to my personal data. Every European citizen is allowed to do so under EU data protection law, yet very few actually do, according to Tinder.

With the help of privacy activist Paul-Olivier Dehaye from personaldata.io and human rights lawyer Ravi Naik, I emailed Tinder requesting my personal data and got back way more than I bargained for.

Some 800 pages came back containing information such as my Facebook “likes”, links to where my Instagram photos would have been had I not previously deleted the associated account, my education, the age-rank of men I was interested in, how many Facebook friends I had, when and where every online conversation with every single one of my matches happened … the list goes on.

“I am horrified but absolutely not surprised by this amount of data,” said Olivier Keyes, a data scientist at the University of Washington. “Every app you use regularly on your phone owns the same [kinds of information]. Facebook has thousands of pages about you!”

As I flicked through page after page of my data I felt guilty. I was amazed by how much information I was voluntarily disclosing: from locations, interests and jobs, to pictures, music tastes and what I liked to eat. But I quickly realised I wasn’t the only one. A July 2017 study revealed Tinder users are excessively willing to disclose information without realising it.

Inside Facebook's suicide algorithm: Here's how the company uses artificial intelligence to predict your mental state from your posts

Benjamin Goggin, Business Insider US

January 6, 2019

Facebook automatically scores all posts in the US and select other countries on a scale from 0 to 1 for risk of imminent harm. Hollis Johnson/Business Insider

- Facebook is scanning nearly every post on the platform in an attempt to assess suicide risk.
- Facebook passes the information along to law enforcement for wellness checks.
- Privacy experts say Facebook's failure to get affirmative consent from users for the program presents privacy risks that could lead to exposure or worse.

Privacy

Individuals need to have the right to privacy and protect their personal information from misuse. Personal data protection is about safeguarding this right to privacy.

In Singapore, data privacy is provided by the *Personal Data Protection Act 2012 (PDPA)*, which aims to provide a minimum standard relating to the collection, use and protection of person data.

Legislation

REPUBLIC OF SINGAPORE

GOVERNMENT GAZETTE

ACTS SUPPLEMENT

Published by Authority

NO. 25] FRIDAY, DECEMBER 7 [2012

First published in the Government *Gazette*, Electronic Edition, on 3rd December 2012 at 5:00 pm.

The following Act was passed by Parliament on 15th October 2012 and assented to by the President on 20th November 2012:—

PERSONAL DATA PROTECTION ACT 2012

(No. 26 of 2012)

Purpose of Act

"The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the *right of individuals* to protect their personal data and the *need of organisations* to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances."
(*emphasis added*)

– section 3, PDPA

Agenda

- What is Data Privacy
- **What is Personal Data**
- Data Protection Obligations
- GDPR Highlights

What is Personal Data

Generally, there is a wide range of opinion what constitutes "personal information":

- Gender
- Name
- Marital Status
- Home Address
- Nationality
- Contact Number (Home)
- Ethnic Origin
- Date of Birth
- Religion
- Political Orientation
- Family / Dependent Information
- Job Title
- Education History
- Company Name
- Employment History
- Office Address
- Financial Information
- Medical/Health Records
- Monthly Salary
- Criminal Records

PDPA Interpretation

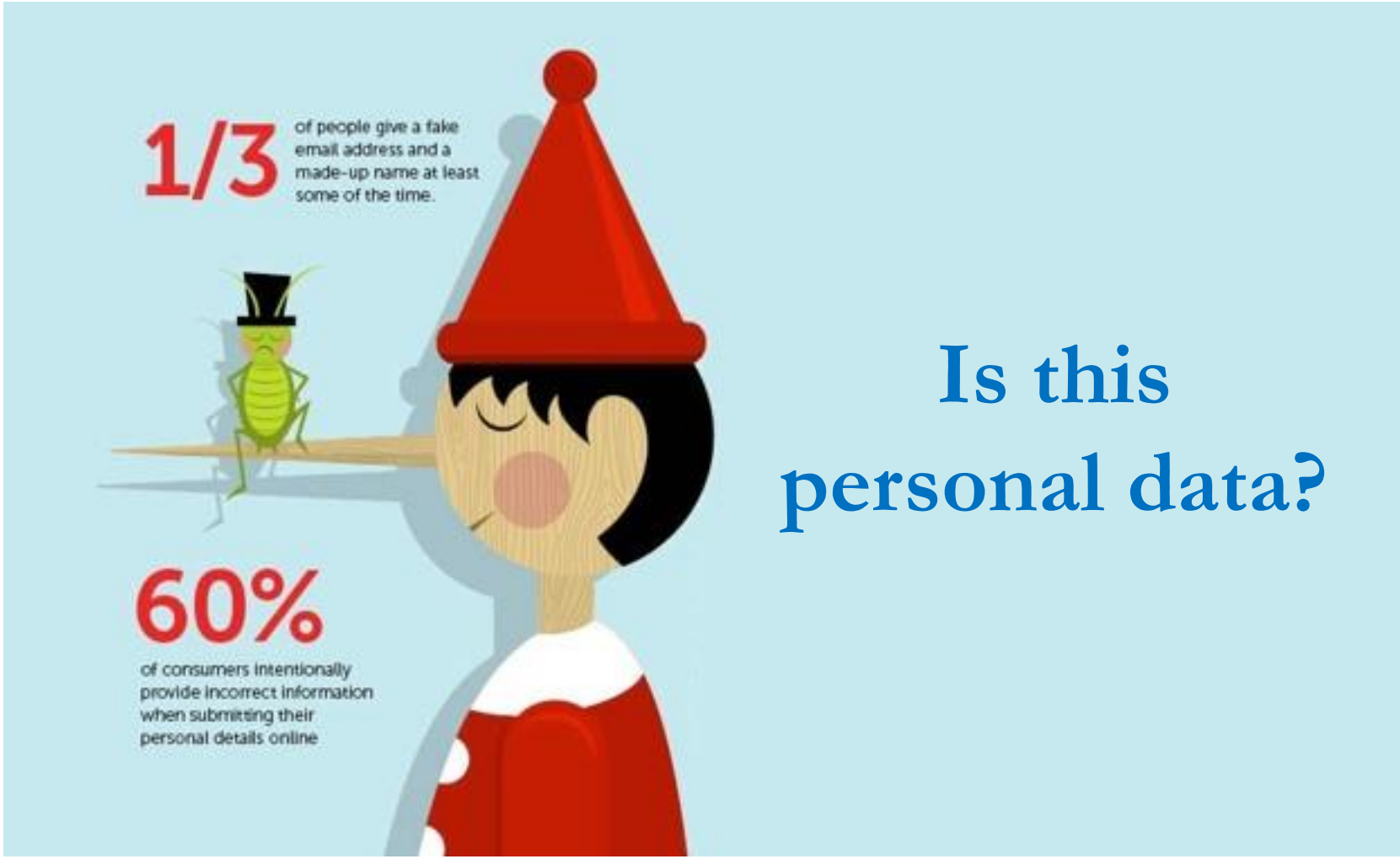
"*personal data*" means data, whether true or not, about an individual who can be identified –

(a) from that data; or

(b) from that data and *other information* to which the organisation *has or is likely to have access*; (*emphasis added*)

– section 2.1, PDPA

Question



Agenda

- What is Data Privacy
- What is Personal Data
- ➢ **Data Protection Obligations**
- GDPR Highlights

What PDPA Provides For

1. Personal Data Protection Commission (PDPC)

- *Statutory Board* established 2 January 2013
- Administer and enforce PDPA
- Public education to help organisations comply with PDPA
- Promote awareness of personal data protection

2. Do Not Call (DNC) Register

- Effective 2 January 2014
- *Individuals can opt out* of unsolicited marketing calls, messages and faxes to Singapore telephone numbers

3. Personal Data Protection

- Effective 2 July 2014
- Recognises *rights of individuals* to protect their personal data
- Recognises *responsibilities of private organisations* to collect, use or disclose personal data for legitimate and reasonable purposes

Obligations

1. Consent
2. Purpose Limitation
3. Notification
4. Access and Correction
5. Accuracy
6. Protection
7. Retention Limitation
8. Transfer Limitation
9. Openness

① Consent Obligation

- **Seek consent from individual for the collection, use or disclosure of personal data**
- **Individual must have been notified the purpose, otherwise any "consent" given would not amount to consent**
- **No misleading / incomplete information**
- **"Deemed consent"**
  - Individual, without actually giving consent, voluntarily provides the personal data to an organisation
  - When the organisation discloses the personal data to another organisation for the same purpose, individual is deemed to have given consent to the second organisation
- **Withdraw consent**
  - at any time
  - after giving reasonable notice

② Purpose Limitation Obligation

- Specify purpose for the collection, use and disclosure
- Purpose considered appropriate by a “reasonable person”

③ Notification Obligation

Inform individual

a) the purpose for the collection, use and disclosure of personal data, on or before collecting the personal data; or

b) any purpose for use or disclosure of personal data which has not been informed under a), before such use or disclosure of personal data for that purpose

Question

PERSONAL DATA PROTECTION POLICY

This Personal Data Protection Policy applies only to the Site, and not to the collection and use of personal data by any third party via any such third party website to which there are links on this Site.

This Site and all personal data collected from users of this Site, are owned solely by [redacted]. In this Condition, references to “we”, “us”, “our”, are references to [redacted].

[redacted] takes the privacy of all our users seriously. We are committed to ensuring that we maintain and protect your personal data in a lawful and responsible manner. Our Personal Data Protection Policy is consistent with the Personal Data Protection Act 2012 (“PDPA”). Our Personal Data Protection Policy outlines how we treat your personal data, and forms part of the Conditions of this Site.

Your use of the Site signifies your consent to us collecting and using personal data about you in accordance with this Personal Data Protection Policy.

Please review the following carefully:

WHAT INFORMATION DO WE COLLECT?

You may access the Site’s home page and browse the Site without disclosing any personal data. In order to provide you with a range of services, however, we may collect your personal data from this Site, from written information sent to us and from other communications. We may for example, keep a record of your name, mailing address, e-mail address, telephone number, gender and preferences.

HOW DO WE USE YOUR INFORMATION?

Any personal data relating to you will be used and recorded by us in accordance with the PDPA and this Personal Data Protection Policy. We may use your personal data to communicate with you, such as to let you know about new features or offerings on the Site ([redacted]) for record keeping purposes, and in aggregate (and therefore anonymously) for market research purposes, to track activity on our Site, to publish trends and/or to improve usefulness and content and for any other purpose that we may notify to you and the relevant data protection authority from time to time.

We may operate a mailing list to send you related news about [redacted]. This mailing list currently operates as a ‘opt in’ mailing list whereby subscribers add themselves to the list. We only send e-mails to addresses which have been subscribed to the list, we do not ‘spam’. If you wish to unsubscribe from the list, please e-mail to enquiries@[redacted]. We do not share, licence or sell these e-mail addresses.

Question

Privacy Policy

1. Acceptance of Policy

1.1 This privacy policy (“Policy”) applies to your access to and use of the InSing/Hungrygowhere/TableDB/Reserveit.sg website (the “Site”) or mobile apps (the “App”) operated or provided to you by or for and on behalf of SingTel Digital Media Pte Ltd (“STDM”), which is part of the SingTel Group.

1.2 You shall be deemed to have agreed to this Policy if you access or use any of the Site or App. If you do not agree to this Policy, you shall not be permitted to and shall not access or use the Site or Appand you must immediately cease any access to or use of the Site or App.

1.3 STDM may modify this Policy at any time at its sole discretion, and such modifications shall be effective immediately upon posting of the modified terms. Your continued access to or use of the Site or App shall be deemed to be your conclusive acceptance of such modified Policy.

2. Collection of Your Information

2.1 When you access or use a Site or App, we may collect the following information:

- personal information which is of a personal nature and may be used to identify you as an individual, and provided by you to us, including but not limited to your name, contact number, email address, mailing address and billing information ("Personal Information"); and
- other information involving you, including but not limited to anonymous statistics, records and other information in relation to your browsing of the Site or App ("Non-Personal Information").

2.2 …

3. Use of Your Information

3.1 You agree and acknowledge that we may use your Personal Information and share your Personal Information with any of our affiliated companies for the purposes of:

- Provisioning & administration essential to the operation of the Site or App
- Providing you with personalised information and recommendations when using the Site or App. The use of your location for recommending nearby restaurants
- Enable the use of social interaction on our websites or mobile apps – eg allowing you to follow other users, reviewing a restaurant or commenting on a news article
- Use of your personal data in an anonymised fashion for data analytics to help improve our services
- …

④ Access and Correction Obligations

- **Verification before granting access**
- **Access to:**
  - personal data in the organisation's possession or under its control
  - Information about ways the personal data has been or may have been used or disclosed within a year before the request
- **Access not permitted where data could reasonably be expected to:**
  - threaten the safety or physical or mental health of an individual other than individual who made the request
  - reveal personal data about another individual
  - reveal the identify of another individual who has provided the personal data, and the individual has not consented to the disclosure of his or her identity
  - be contrary to national interest
- **Respond to the error or omission**
- **Send the corrected data to every other organisation to which the personal data was disclosed by the organisation**

Question

What if organisations:

- do not know what personal data they have?
- how they have used it?
- who they have disclosed it to within the last year?
- can no longer charge a ‘reasonable’ fee for an Access request?
- have only 30 days to respond to an Access request?
- have to provide the personal data in a commonly used and machine-readable format?

⑤ Accuracy Obligation

- Ensure that personal data collected by, or on behalf of the organisation, is accurate and complete
- Personal data may change over time; organisations can assume accuracy of personal data as at time of correction
- Good practice to periodically validate currency of personal data where it is used for decision-making that affects the individual

⑥ Protection Obligation

- **Protect personal data against**
  - Accidental or unlawful loss
  - Unauthorised access
  - Disclosure or copying
  - Use or modification
- **Some methods of protection**
  - Physical measures, e.g., secured filing cabinets, restricted access…
  - Organisational measures, e.g., security clearance, limited access…
  - Technological measures, e.g., use of password, encryption…
- **Extents and scope of safeguards depending on**
  - Sensitivity of the data
  - Amount, distribution and format of the data
  - Method of storage
  - Technology availability

⑦ Retention Limitation Obligation

- **Only for period necessary for the fulfilment of the purpose**
- **Destroy or remove the documents if:**
  - the purpose for which that data was collected is no longer being served by retention
  - retention is no longer necessary for legal or business purpose
- **An organisation is considered not to retain personal data when it no longer has the means to associate the personal data with particular individuals, i.e., the personal data has been anonymised**

⑧ Transfer Limitation Obligation

- **Responsibilities remains even when personal data is situated outside Singapore**
- **Requirements before transferring out:**
  - Laws of the country to which the personal data is transferred provides similar protection
  - Contractual obligations with recipients
  - Consent from owner of personal data

Question

The Regulatory Landscape

Overview

As in many countries, the pace of cloud adoption in Singapore has, in the past, been hampered by concerns about the regulatory environment. The concerns focused, in particular, on the ability of cloud services providers to ensure compliance with a high level of security and privacy. This was a particular issue in highly-regulated sectors such as financial services, education, healthcare and the public sector. That has now changed as various new regulations and guidance across sectors make it clear that organizations can move to the cloud in a way that meets all applicable security and privacy requirements. Indeed, cloud services from leading providers such as Microsoft are now recognized for their ability to offer levels of security and privacy compliance that exceed those available via on-premises solutions of even the most sophisticated organizations. As a result of these developments, Singapore is regarded as one of the most innovation-friendly environments in the region for the adoption of new technologies such as cloud computing.

At Microsoft, we welcome these positive developments, which have brought greater clarity to the regulatory requirements for the adoption of cloud. In fact, we are pleased to have already participated in a large number of compliance conversations with customers and regulators across sectors, from becoming the first global cloud services provider to receive a certification across all three classifications under IMDA's Multi-Tier Cloud Security (MTCS) Standard though to partnering with major Singapore organisations such as DBS Bank on their procurement of cloud. Through these conversations, we have developed a broad range of materials to help our customers move to the cloud in a way that meets applicable regulatory requirements in Singapore, such as product checklists, which map Microsoft's cloud services against the underlying regulations, so that organizations can be confident that their use of Microsoft cloud services meets the necessary requirements. We are delighted to share these materials via this guide.

Other Resources

Personal Data Protection Act 2012 ›

Review the original legislation which regulates personal data and privacy in Singapore.

ISO/IEC 27018 Privacy Snapshot: Singapore ›

Follow this link to read more about how [redacted] compliance with and certification of ISO/IEC 27018 in Singapore enables your organization to continue to comply with the relevant obligations in Singapore's privacy law.

Compliance is not Vendor's Responsibility

Customer's PDPA obligations	Does ISO/IEC 27018 help compliance? How?
Consent and Purpose Generally, a cloud customer must obtain the consent of a data subject in order to collect and process personal data and must only use the personal data for the purposes for which it was collected (Section 13).	**Yes** ISO/IEC 27018 requires the CSP to process personal data in accordance with the cloud customer's instructions and prohibits processing for any other purposes (A.2). The obligation to obtain consent remains the cloud customer's responsibility.
Sub-contracting The cloud customer may use subcontractors to process personal data on its behalf as long as the cloud customer ensures that the personal data is protected to the same level as required by the PDPA (Section 4).	**Yes** ISO/IEC 27018 requires the CSP to execute a contract with any sub-contractors that includes the same security and personal data protection obligations of the CSP (A.10.12).
Data subjects' right of access and correction The cloud customer must, upon request, provide access to and/or correct the data subject's personal data (Sections 21 and 22).	**Yes** ISO/IEC 27018 requires the CSP to assist its cloud customer to comply with a data subject's access and/or correction requests (A.1).
Security The cloud customer must make reasonable security arrangements to prevent unauthorized access, collection, use or disclosure, of personal data (Section 24).	**Yes** ISO/IEC 27018 requires the CSP to implement security measures to prevent unauthorized access, collection, use or disclosure, of personal data (5 to 13 and A.10).
Data retention A cloud customer must retain personal data only for as long as is necessary to fulfil the purpose for which it was collected (Section 5).	**Yes** ISO/IEC 27018 requires the CSP to implement a policy to erase personal data when it is no longer required by the cloud customer (A.9.3).
International transfer A cloud customer may transfer personal data outside of Singapore if the personal data is treated to a standard of protection that is comparable to the PDPA (Section 26).	**Yes** ISO/IEC 27018 requires the CSP to apply the same exacting standards to the personal data, no matter where the personal data is processed (Generally and A.11).

⑨ Openness Obligation

An organisation:

a) Is responsible for personal data in its possession or under its control

b) Shall develop policies and practices for data protection

c) Shall make openly available such policies and practices

d) Shall delegate one or more individuals to be responsible for ensuring that the organisation complies with this Act

e) Shall make available to the public the business contact information of at least one of the individuals designated under b) above

Agenda

- What is Data Privacy
- What is Personal Data
- Data Protection Obligations
- **GDPR Highlights**

EU GDPR

- **The European Union (“EU”) General Data Protection Regulation (the “GDPR”) was adopted on 14 April 2016 and came into force on 25 May 2018**
- **The GDPR unifies data protection laws across the EU and has global reach in protecting the personal data of EU citizens**
- **The GDPR applies to all organisations outside of the EU as long as the organisation:**
  1. Offers goods or services to individuals in the EU irrespective of whether a payment is required; or
  2. Monitors the behaviours of individuals with the EU
- **The GDPR provides for penalties of up to 20 million EUR or 4% worldwide annual turnover of preceding year (whichever is higher)**

PDPA Compliance ≠ GDPR Compliance

In summary, organisations need to ensure that internal policies and processes comply with:

1. Consent obtained from data subjects for the processing of his/her personal data is clear and unambiguous. The purpose for obtaining such personal data should be clearly stated
2. Personal data should not be retained longer than is necessary for the purposes for which the personal data was processed
3. Data subjects should have the right to:
   - access and correct personal data concerning him/her
   - withdraw consent to the processing of his/her personal data at any time, and such withdrawal of consent should be as easy to withdraw as it is to give
4. No processing of personal data classified as ‘special’ under the GDPR (i.e., racial, ethnic origin, sexual orientation, philosophical beliefs) unless the limited exemptions under Article 9(2) of the GDPR applies
5. Personal data breaches should be reported no later than 72 hours from the time the breach is discovered. Additionally, the breach and any subsequent remedial actions have to be clearly documented

Fewer Exemptions

The PDPA provides exemptions from data protection obligations to the following entities:

1. employees acting in the course of his/her employment with an organization
2. public agencies
3. any organization acting on behalf of a public agency in relation to the collection, use or disclosure of personal data
4. organizations which are data intermediaries[3] are also partially excluded from the provisions under the PDPA

By contrast, the GDPR applies so long as an individual or entity (including a public authority or agency) falls within the definition of 'data controller' or 'data processor' under Article 4 of the GDPR.

THANK YOU

nicholas_tan@nus.edu.sg