LEGAL ASPECTS OF INFORMATION SECURITY IFS4101

WEEK 11, WELLY TANTONO, DIS, SOC, NUS

WHAT IS PERSONAL DATA?

"PERSONAL DATA" SECTION 2 PDPA

- "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;
- "individual" means a natural person, whether living or deceased;

"PERSONAL" DATA

- Data "about" individual
- Examples of personal data (direct identification)
  - Full name
  - NRIC Number or FIN (Foreign Identification Number)
  - Passport number
  - Personal mobile telephone number
  - Facial image of an individual (e.g. in a photograph or video recording)
  - Voice of an individual (e.g. in a voice recording)
  - Fingerprint
  - Iris image
  - DNA profile
  - Residential address (but see PDPC Guidelines, Para 5.5, Why?)
- Examples of personal data (indirect identification)
  - Blood type
  - Occupation
  - Educational institutions

"PERSONAL" DATA

- Who is this "individual"?
- What data is "about" an individual (vs. data that "relates to" an individual)? (See assigned reading Chik, 380-391)
  - "About" is info to identify w/o reference to other info – "Relates to" is any info about that individual; cf. any info that "affects his privacy"
  - EC Article 29 Data Protection Working Party: **content, purpose and result** as the test of whether or not data "relates" to an individual.
- How is an individual "identified" from the personal data?
  - Identification by "singling out" the individual from other individuals based on one or more characteristics of the data (PDPC Guidelines, Para 5.9)
  - Direct and indirect identification (based on certain data and other information) (PDPC Guidelines, Para 5.10); question of the likelihood of such indirect identification

"PERSONAL" DATA

- "publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event —
  a) at which the individual appears; and
  b) that is open to the public;
- Why does PDPA, First Schedule (Part 2, Paragraph 1), provide that an organisation may collect personal data about an individual where the personal data is publicly available (without the individual's consent)?
- If data about an individual is on the Internet, does this data cease to be "personal data"? Is there "public" personal data?

"BUSINESS" PERSONAL DATA

- Business contact information is excluded as "personal data"
- Defined as "***individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes***"
  - Cf. what about "dual use" information e.g. mobile number?
- IS issues: "confidentiality" - business contact information to be marked "non personal data"?
- "access" – unrestricted access allowed?

WHAT IS DERIVED PERSONAL DATA?

- "derived personal data" —

  a) means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; but

  b) does not include personal data derived by the organisation using any prescribed means or method;

- Provide examples of data sets that can be gathered without consent because it was "publicly available"
- If data about an individual is on the Internet, does this data cease to be "personal data"? Is there "public" personal data?
- Can an organisation, organisation A, use "publicly available" personal data by first making them publicly available?
- Can organisation B use personal data that organisation A has made "publicly available"?
- How would one store information about a person in a system that allows the management of the contact information about a person to take into account whether the information was publicly obtained, was given by the individual as "personal data" or given out as "business contact information"?
- If you can collect publicly available information under the PDPA, does that mean you can send them marketing materials?

SMALL GROUP DISCUSSIONS

(20 MINUTES)

EXTRA-TERRITORIALITY

- Does the PDPA apply to
  - Personal data of individuals not in Singapore?
  - Organisations not in Singapore?
  - Intermediaries not in Singapore?
- Extraterritoriality of application part of modern data protection legislation to regulate transborder data flows
- IS issues:
  - "access" - authorising transborder data flows to permissible third party organisations, or limiting unintentional transborder data flows e.g. cloud computing
  - What controls will you need to implement to ensure that trans-border flows are compliant to the PDPA?

DATA ORGANISATIONS AND INTERMEDIARIES

DATA ORGANISATION: PDPA SECTION 2

- "organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not —
  a) formed or recognised under the law of Singapore; or
  b) resident, or having an office or a place of business, in Singapore;
- Exempted:
  - Individuals acting in a personal or domestic capacity
  - Employees acting course of employment with organisation
  - Public agencies
- **Question: What is the rationale for excluding public agencies from the PDPA?**

WHO IS A "DATA INTERMEDIARY"?

- A "data intermediary" as a "network service provider" with no liabilities under the PDPA: s 26(1A) of the Electronic Transactions Act
- A "data intermediary" as a special "data organization" with limited PDPA obligations
- PDPA, s 2
  - "data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;
- **Question: How is the definition of a "data intermediary" helpful in describing what a "data organisation" is?**

PRINCIPLES OF DATA PROTECTION

CONSENT AND PURPOSE

Sections 13 and 20, PDPA

An organisation shall not "use, collect or disclose personal data about an individual" unless the individual has "been notified of the purpose for which the personal data is to be collected, used or disclosed" and provided consent for that purpose,

PRINCIPLES OF DATA COLLECTION

- consent
- limited purpose
- right of access
- right of correction
- accuracy and completeness
- security
- cessation of retention
- no unrestricted transborder transfers
- data portability (not yet implemented)

"REASONABLE" STANDARDS

- Compliance with PDPA is based on "reasonableness":
- "In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances." – section 11(1), PDPA
- What is "reasonable" will depend on an objective evaluation of the circumstances, not a subject evaluation of the situation of the organization.
- IS: industry standards or benchmarks, best practices as helpful, but not authoritative, guides to "reasonableness"

WHAT IS REASONABLE FOR THE FOLLOWING SITUATIONS … (25 MINS)

- **Case A:** USD 5 billion multinational corporation headquartered in New York, New York, that makes furniture and sells furniture and buys customer data from marketing agencies for the purposes of sending promo codes and other advertisements. Does not collect customer data other than what is necessary to send the goods to the customer.
- **Case B:** Singapore-based start up that runs a social media application that collects and sells the profiles of the users of its applications to advertisers. Has a capitalisation of SGD1,000,000; founders are not paid.
- **Case C:** A voluntary welfare organisation (VWO) that matches doctors to low-income patients and survives mainly on donations. To make sure that the patients remember their doctors, the organisation keeps a spreadsheet that shows the names of the patients, their contact information, the names of their doctors, the doctors' specialisations and the reason that the organisation matched a patient to a particular doctor. The VWO has very little resources and relies on volunteers to help maintain the database and do the matching.
- **Case D:** A hawker who sells nasi lemak and takes orders for pick-up and delivery using food delivery apps and also their own mobile lines. Customer calls are logged using the mobile lines. Hawker cycles through temp helpers to manage food orders.

Each group to answer the following questions:

1. Based on your gut feel, rank the cases in **decreasing** order of the extent to which each organisation must implement safeguards to comply with the PDPA.
2. Identify the factors will be used to determine whether or not a data organisation is likely to be found to have acted in a reasonable or not reasonable based on the different scenarios.

IMPLEMENTATION DETAILS

- Appointment of Compliance Officer/Data Protection Officer – responsible for organisation's PDPA compliance: s 11(3), PDPA
- New policies and practices to be developed: s 12(a), PDPA
- Communicate to its staff information about the organisation's policies and practices (i.e., training, educating, awareness): s 12(c), PDPA
- Policies and practices to be "made available ... on request": s 12(d), PDPA

IMPLEMENTATION DETAILS

- Some suggested steps:
  - inventory map to determine what personal data is held
    - nature of personal data
    - sources of personal data
    - purpose for which personal data is held
    - use of personal data
    - disclosures of personal data
  - aligning IT system or infrastructure
    - compatibility between PDPA obligations and business operations
  - audits of organisation, including security audits

CONSENT AND OPTING IN VERSUS OPTING OUT

CONSENT AND DATA PROTECTION

- Consent prescribed in PDPA, Sections 13, 14, 20
  - consent to be "informed": individual to be told about
  - purpose, "on or before" collection, use and/or disclosure
  - consent to be uncoerced and not misguided – no "tricks"

CONSENT AND DATA PROTECTION

- IS: How is consent recorded? Where is it recorded?
- **Question:** A corporation is attempting to verify the particulars of the subscribers of its newsletter. To do this, it sent out a circular to all its subscribers based on their currently provided names and addresses. The circular said, "We would like you to mail us back with the return-provided card if you like to continue to receive more issues of this newsletter." Is this an attempt to mislead to collect personal data? Why? Why not?

COMPARE THE TWO SCENARIOS (GROUP DISCUSSION 10 MIN)

Scenario 1

Retailer A has collected personal data from its customers for the purpose of delivering products purchased by the customers. It subsequently mails a flyer to the customers which states that a customer would have consented to the disclosure of his personal data to Company Z to market the products of Company Z unless the customer writes back to the retailer to opt out by a certain date. Company Z receives no response from the customer.

Scenario 2

Retailer B puts up a sign informing customers who are interested to join their membership programme to obtain an application form from a shelf next to the counter, fill it out, and drop the completed form into an unmanned box next to the shelf. A line in the form with an accompanying tick box states clearly "tick here if you do not wish your personal data to be provided to Company Z to market Company Z's products". The last field of the form requires the customer to provide his signature. The customer signed the form without putting a tick in the tick box and drops the completed form into the box.

Was consent given in either scenario? Why or why not?

CATEGORIES OF DEEMED CONSENT

- Three types of deemed consent:
  - Conduct-based
  - Contractual-based
  - Notification-based (driven by business needs and consider potential conflict with Section 14's need to obtain consent)

SECTION 15(1): CONDUCT-BASED DEEMED CONSENT

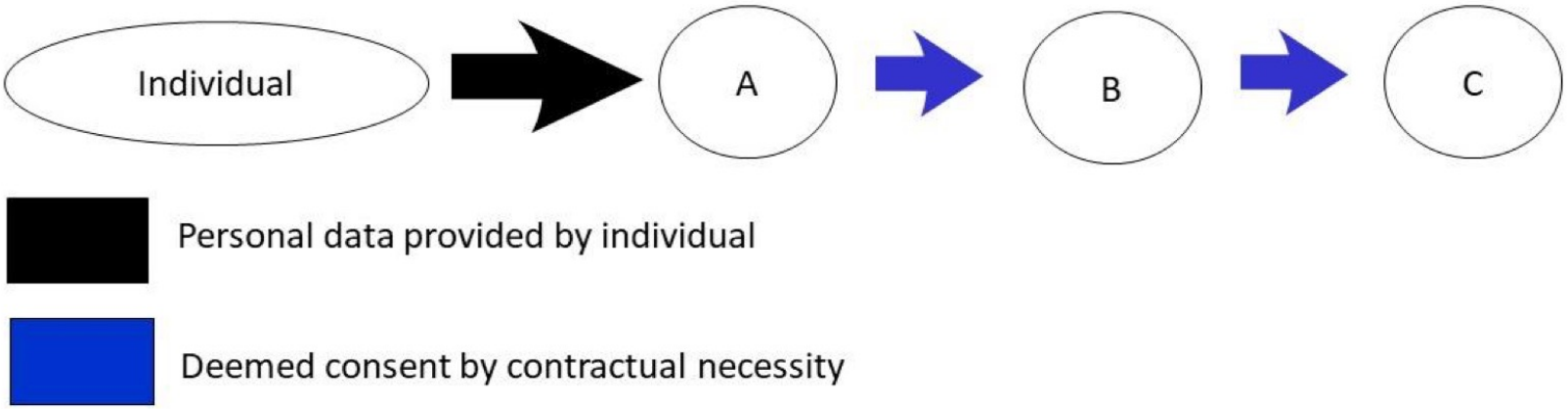
- Consent exists when individual voluntarily provides data
- Use, disclosure and processing and other treatments are **limited to the purpose that is:**
  - objectively obvious
  - reasonably appropriate
- Note that the organisation must make a judgment call on what is objectively obvious and reasonably appropriate
- ***Why is there a need for conduct-based deemed consent?***
- Suppose you run a medical concierge service (i.e., a service that helps customers book appointments with medical institutions).
  - If your customer were request your services online, what would you rely on for consent?
  - If the customer were to request for your services through a telephone hotline, what would you rely on for consent?

SECTION 15(3): CONSENT BY CONTRACTUAL NECESSITY

- When an organisation enters into a contract with a customer, supplier or employee, previously, organisations had to rely on either Section 15(1) (deemed consent by conduct) or implied consent in Section 17 plus the First, Second, Third and Fourth Schedules. However, none of these schedules made clear the level of downstream sharing that would be permitted.
- The concept of consent by contractual necessity boils down to the recognition of modern businesses:

  "*Multiple layers of contracting and outsourcing are common in modern commercial arrangements. … expands deemed consent to cater for scenarios where personal data is passed from an organisation to* ***successive layers of contractors*** *for the organisation to fulfil the contract with its customer.*"
- Crucially, Section 15(2) still applies – i.e., use, disclosure and processing and other treatments are **limited to the purpose that is:**
  - objectively obvious
  - reasonably appropriate

SECTION 15(3): CONSENT BY CONTRACTUAL NECESSITY



SECTION 15A: DEEMED CONSENT BY NOTIFICATION

- Consent by notification allows organisations to notify their customers of the new purpose, give them a reasonable period to opt out, and, if the organisation doesn't get an active opt-out, they are allowed to assume that the customer has consented.
- *Why do you think businesses wanted this to be made into law?*
- How does this work?
  - Must conduct a risk assessment
  - Must conclude that the collection, use or disclosure of personal data in this manner will **not likely have an adverse effect** on the individual.
- Safeguards to be implemented by the PDPC
- Deemed consent by notification **not permitted for direct marketing messages**

COLLECTION, USE AND DISCLOSURE WITHOUT CONSENT AND DATA PROTECTION (FIRST SCHEDULE)

- In interest of individual
- Emergencies
  - Threats to life, health, safety of individual or another
- Reasonable grounds to believe health and safety will be affected and consent cannot be obtained timely
- Contacting next-of-kin or friend of injured, ill or deceased
- Publicly available
- National interest
- Artistic or literary purposes
- Archival or historical purposes
- News activity
- Legitimate interests of the organisation that outweigh adverse effect on individual
- "Evaluative purposes"
- Investigation or proceedings for debt recovery or to pay
- Legal services
- Credit bureaus
- Trust/benefit
- Provided by another individual to provide a service to the data subject
- Employment, business or profession
- Employment and termination
- Business asset transaction
- Business improvement

ADDITIONAL BASES FOR COLLECTION, USE AND DISCLOSURE WITHOUT CONSENT (SECOND SCHEDULE)

- Collection of data if it was disclosed by a public agency and collection is consistent with the purpose of disclosure
- Use of data if it was disclosed by a public agency and use is consistent with the purpose of disclosure
- Business use to:
  - Improve/enhance goods/services
  - Improve/enhance methods or processes for operations
  - Learning and understanding behaviour and preferences in relation to goods/services
  - Identifying/personalizing/customizing (i.e., recommendation engine)
- Research use
- Disclosure to a public agency in the public interest
- Disclosure to a public agency for the purposes of education policy formulation or review
- Disclosure to public agency for the purposes of health policy formulation or review
- Disclosure to law enforcement
- Disclosure for research purposes

FIRST AND SCHEDULES (KEY EXCEPTIONS TO CONSENT)

- **Legitimate business interest.** Reliance on this exception requires organisations to:
  - conduct an assessment to eliminate or reduce risks associated with the collection, use or disclosure ("CUD") of personal data, and
  - assessment must satisfactorily conclude that the overall benefit of CUD outweighs any residual adverse effect on an individual.
  - Disclose when they rely on this exception.
  - *Consider anomaly detection in payment systems to prevent fraud or money-laundering. Do you think that this activity could have been conducted without obtaining the customer's explicit consent any other way?*

FIRST AND SCHEDULES (KEY EXCEPTIONS TO CONSENT)

- **Business improvement purposes.** The purpose of this exemption is to enable operational efficiency and service improvements; develop or enhance products or services; and to get to know the organisation's customers.
  - This exception is available only for:
    - purposes that a reasonable person may consider appropriate in the circumstances and
    - where the purpose cannot be achieved without the use of the personal data.
  - Available to entities within a group to enable consolidation of R&D functions within large organisations (frequently R&D is a separate legal entity than the sales units in Singapore) Intra-group sharing requires inter-company contracts or binding corporate rules.
- **Research purpose.** Specifically allows CUD without consent to conduct commercial research and development that is not immediately directed at productisation. This could apply to research institutes carrying out scientific research and development, educational institutes embarking on social sciences research, and organisations conducting market research to identify and understand potential customer segments.

WITHDRAWAL OF CONSENT

- Section 16(1): Consent can be withdrawn for "express" and "deemed" consent (but not for collection, use and disclosure "without consent" as required or authorized under the Act)
- Section 16(3): Organisation not to prohibit individual from withdrawing consent
- IS: "integrity" – alterations to be made to individual personal data within database (not necessary to delete records – PDPA) – See Advisory Guidelines, para. 12.54
- Advisory Guidelines, para. 12.52-12.53): Need to ensure that the data organisation and its data intermediaries are compliant with the withdrawal request, but no need to inform other organisations to whom the data organisation has disclosed personal data. However, data organisation may need to disclose the ways in which personal data may have been disclosed to third parties so that the data subject can give notice to withdraw consent to those third parties.

LIMITATION OF PURPOSE

DATA PROTECTION OBLIGATIONS: LIMITATION OF PURPOSE

- Section 18 of the PDPA makes clear that any collection, use or disclosure (CUD) must be limited to:
  - purposes "that a reasonable person would consider appropriate in the circumstances, [AND]
  - that the individual has been informed [of the purpose under section 20] if applicable"
- Purpose need not be disclosed where personal data is collected, used or disclosed under the deemed consent regime established in Sections 15 and 15A or for CUD permitted "without consent" under Section 17 and the First and Second Schedules

EMPLOYEE INFORMATION

EMPLOYEE INFORMATION

- The treatment of employee information, before the PDPA, was always rather fraught. Unless an organisation is in a sector like financial services, communications or healthcare, organisations don't usually have access to extremely sensitive information.
- However, employee information is a different matter. The collection of employment-related information starts from pre-employment, throughout employment and even post employment and includes highly sensitive data. These are:
  - Bank information
  - Family relationship
  - Health information
  - Evaluation information
  - Information obtained from investigations
  - Personal correspondence (e-mails, voicemail, instant messages)
- Some of the collection of employment information is required under the laws. Others are part of the company's process of placing controls on their insurance premiums, for management of employees, etc.

EMPLOYEE INFORMATION

- Section 20(3) exempts organisations from the notification obligation under Section 20(1) where consent is deemed to have occurred under Sections 15 or 15A, or where CUD is allowed without consent under Section 17
- CUD of employee information is permitted to occur without consent under Section 17 and the First Schedule. However, for CUD of employee information, organisations must inform the individual of the:
  - Purpose of CUD
  - The business contact of the person who can answer questions about the CUD

  ON OR BEFORE
  - Entering into an employment relationship or appointing person to any office
  - Managing or terminating the employment relationship with or appointment of the individual
- *Why is there a need for a provision that gives employee rights?*
- *Can employers simply put a generic "employee deemed informed" provision in the employment contract?*
- *What about collection of information on the personal devices belonging to employees?*

PART 5: ACCESS TO INFORMATION

- Section 21 guarantees the right of access to personal data
  - Only to the data in the possession or under the control of the organisation – in other words, if your organisation has transferred the data to a data intermediary, the organisation must still provide access to the data that is in the data intermediary's possession.
  - Organisation may limit the access to information that has been or may have been used or disclosed by the organisation within a year before the date of the request.
  - There are exceptions to the access rights – specifically, under Section 21(3), (4) and Fifth Schedule. Moreover, if organisation refuses to provide data, must preserve that data under Section 21A.

Does the data intermediary have an obligation to provide access to personal data since the data is in the intermediary's possession?

- Information Security standpoint:
  - "confidentiality" – segmentation of personal data by individuals;
  - "integrity" – meta data to be kept about usage/disclosure of data

PART 5: CORRECTION OF PERSONAL DATA

- Section 22 gives the data subject the right to seek the correction of errors or omissions in personal data
  - Section 22(2) allows the organisation not to correct the data if it can establish reasonable grounds to not correct the data (e.g., the request for correction is itself erroneous)
  - Once the organisation decides to correct the data, must send corrected personal data to every other disclosed organisation
- Information Security standpoint:
  - "integrity" – relaxed to permit modifications; meta data used to track organisations to whom modified personal data is to be sent

PART 5: PRESERVATION OF COPIES OF PERSONAL DATA

- Section 22A establishes what happens if an organisation refuses to produce the personal data as permitted under Sections 21(2) and 21(3).
- Even when an organisation is allowed to withhold access to personal data that has been collected, the organisation must still:
  - preserve, for not less than the prescribed period, a copy of the personal data concerned.
  - The organisation must ensure that the copy of the personal data it preserves for the purposes of subsection (1) is a complete and accurate copy of the personal data concerned.

PART 6: CARE OF PERSONAL DATA

- Section 23: Obligation to ensure data is accurate and complete:
- Section 24: Obligation to secure data: PDPA
  - Information security standpoint: intersects with the "confidentiality" and "integrity" aspect of IS; implementation through encryption
  - Take note that this obligation applies to data intermediaries
- Section 25: Obligation to not retain personal data if purpose is not served and retention not legally needed
  - Take note that this obligation applies to data intermediaries
  - Information security standpoint: "access" – alteration of privileges once purpose is no longer served but data is not being deleted because there may be a need to hold the data for legal purposes

PART 6: CARE OF PERSONAL DATA

- Section 26: Obligation not to transfer data overseas unless they provide a standard of protection to the transferred data that is comparable to the protection under the PDPA.
  - Information Security standpoint:
    - "access" – meta data/geolocation information/information to characterise data protection status of jurisdictions
    - How do you propose handling the oversight of information overseas?
    - Examples of overseas transfers that need to be compliant to the PDPA:
      - Transfers to another company within the same group for centralised corporate functions
      - Transfers to data intermediary for data processing
      - Employee travels overseas with customer lists on his notebook
      - Data is transferred to overseas physical or data warehouse overseas for archival of records

DATA TRANSFER OVERSEAS

- To ensure that data transfers overseas are compliant to the PDPA, an organisation must do one of the following:
  - Ensure that overseas laws provide equivalent or better protection (this will require organisations to monitor overseas regulations, which can be tedious).
  - Enter into contracts that impose a standard of protection that is comparable to that under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract.
  - Adopt binding corporate rules that require every recipient of the transferred personal data to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA,. See PDPC Advisory Guidelines 19.5
  - Any other legally binding instrument (e.g., oath, declaration, etc.)

DATA TRANSFER OVERSEAS

- The transfer limitation obligation is satisfied if the recipient holds a valid Asia Pacific Economic Cooperation Cross Border Privacy Rules ("APEC CBPR") System certification or, if the recipient is a data intermediary, if it holds either a valid APEC CBPR or a valid Asia Pacific Economic Cooperation Privacy Recognition for Processors ("APEC PRP") System certification
- Data in transit is automatically deemed to comply with the transfer limitation obligation. See Advisory Guidelines, para. 19.11.
- GDPR-compliant transfers also have the same concepts but will require the entry into "Standard Contractual Clauses" that have substance of the form given in the EU regulations.
- **How do you deal with the modern business practices where so much processing of personal data is being handled by vendors? Can you identify the questions you need to ask the vendors to ensure that your organisation will remain compliant with the data transfer limitations established by the PDPA?**


10:00