NATIONAL UNIVERSITY OF SINGAPORE

IFS 4101 – LEGAL ASPECTS OF INFORMATION SECURITY

AY2021/2022, Semester 2, Weeks 11-12

PERSONAL DATA PROTECTION ACT 2012

I. WHAT IS PERSONAL DATA?

The object of the PDPA is to protect data about natural persons or "personal data". Corporations have no "personal data", but, in many countries, the employees of corporations have "personal data" in the form of their business email addresses, business telephone numbers and so forth. In the case of Singapore, "business contact information" is specifically excluded from many of the obligations that apply to the protection of personal data.

According to the Personal Data Protection Commission ("PDPC"), personal data may include the following.

- 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

The PDPC has also produced the following helpful advisory about what constitutes "personal data". In general, whether a piece of data or set of data characteristics is "personal data" depends on the context. For instance, the PDPC has taken the view that a residential address is, on its own, not personal data. But together with other information associated with the address (such as the contact information collected as other data about the individual), the data could be personal data. You should review the Advisory Guidelines on Key Concepts in the Personal Data Protection Act published by the PDPC (revised 1 October 2021) ("Advisory Guidelines") to get a better understanding of what constitutes personal data.

In addition, an individual can be identified from other identifiers relating to the individual, to which the organisation has or is likely to have access, a process known as "data matching".

"Deceased individuals" have some residual personal data protection rights. However, personal data in a record that has been in existence for at least 100 years is outside the scope of the PDPA. See Section 4(4) of the PDPA.

The issue about when data or opinion data can be indirect "personal data" is dealt with in the following article: Warren Chik and Joey Pang, *The Meaning and Scope of Personal Data under the Singapore Personal Data Protection Act* (2014) 26 SAcLJ 354, 377-391 [LINK] (dealing with issues of when data is "about" an individual).

A. Publicly Available Data

Unlike many other countries, the PDPA does not give much protection to "publicly available" data. In particular, if a defendant manages to prove that a particular piece of information was publicly available, that defence is valid against criminal charges brought under Sections 48C – 48E for unauthorised disclosure, improper use and unauthorised re-identification of anonymised information, respectively. In addition, Part 2 of the First Schedule, which identifies the circumstances under which the collection, use and disclosure of personal data can be performed without the need for consent, specifically identifies "publicly available" information as falling within the category of data that is not protectible under the PDPA.

Questions:

1. What data about an individual is "publicly available"? Can you provide some examples? Why would such data not be protected as "personal data"? Why not?

2. Which of the following is "publicly available" personal data: (a) a blogger's email and physical address; (b) Facebook posts about the wedding of a couple; and (c) NRIC and mobile numbers of the top contest winners published in the newspapers?

3. Can an organisation that publishes these details use these details because they are consequently publicly available? Can organisation A use the personal data that is publicly published by organisation B for its (organisation A) purposes, without complying with its PDPA obligations?

B. Business Contact Information

Section 4(5) of the PDPA specifically excludes business contact information from the protections given to personal data under Parts 3, 4, 5, 6 and 6A of the PDPA. Section 2 defines "business contact information" to mean "*an 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 or her personal purposes***." See Advisory Guidelines for a greater understanding as to what constitutes business contact information.

Questions:

1. What if the information provided is "dual use" information (e.g., a person provides her business contact information for contact purposes)?

2. What information security and data management issues would be introduced by this qualified definition of what constitutes "personal data"? You may want to think about these problems prospectively and retrospectively. [This will be for the group discussion in class].

C. Extra-Territoriality

Like all modern data protection legislation, the PDPA has extra-territorial application: there is no reference to the need for an individual to have a connection with Singapore.[1] The PDPA applies to all organisations other than those organisations that are exempt under Section 4(1). The definition of the term "organisations" is broad and gives no exemptions based on whether or not the entity involved is "formed or recognised under

[1] Advisory Guidelines, para. 6.2.

the law of Singapore or whether they are resident or have an office or place of business in Singapore."[2]

Does this mean that the PDPA applies to personal data that is collected by foreign entities outside of Singapore and doesn't ever travel across Singapore borders? No, the Advisory Guidelines make clear that the PDPA is meant to apply to collection, use and disclosure of personal data in Singapore. See Paragraph 6.3 of the Advisory Guidelines. Note, however, that this means that a data intermediary located in Singapore, who is processing personal data collected outside of Singapore, must ensure that the treatment of that personal data is compliant to the PDPA, with some exceptions. See the section below concerning data intermediaries.

II. DATA ORGANISATIONS SUBJECT TO PDPA

As mentioned previously, PDPA requires all organisations to comply with their statutory data protection obligations. Section 2 of the PDPA defines "organisations" as "*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[.]"

I will refer to organisations that are subject to the PDPA as "data organisations" throughout this document.

Questions:

1. Is a "partnership" an "organisation" under the PDPA? You may wish to research what a "partnership" means. Go to the ACRA website (**www.acra.gov.sg**) to get a better understanding.
2. Are foreign corporations subject to the PDPA?
3. What about NUSSU?
4. What about a "study group" of students?

A. Exempt Organisations

Section 4(1) of the PDPA exempts the following from the obligations imposed under Parts 3, 4, 5, 6, 6A and 6B of the PDPA:

"*(a) any individual acting in a personal or domestic capacity;*

(b) any employee acting in the course of his or her employment with an organisation;

(c) any public agency; or

(d) any other organisations or personal data, or classes of organisations or personal data, prescribed for the purposes of this provision."

[2] Id.

Any individual acting in a personal or domestic capacity is exempted from the PDPA obligations. These would, for instance, include examples like a husband opening a joint account with his wife, or purchasing a life insurance policy for his children.[3] Likewise, any employee acting in the course of his employment is exempted from the PDPA. However, on the principles of vicarious liability, this does not detract from the fact that the employee's course of conduct may subject the employer to PDPA obligations.[4]

Singapore's PDPA is peculiar in that public agencies are exempted from compliance with the PDPA. Organisations that provide services to public agencies "may have obligations as data controllers or as data intermediaries",[5] although it is not clear what "data controller" means in this regard as the PDPA itself does not define the term "data controller" and the Advisory Guidelines used this term only once in Paragraph 6.14. What is obvious, however, is that all organisations must be responsible for the personal data of its employees and customers. Where the organisation is subject to a contract with a public agency to process data on behalf of that agency, that service provider organisation will be handling the data as a "data intermediary" even though the first point of collection of that data may be through the service provider organisation itself.

Note, however, that organisations that provide services to public agencies may be subject to other laws and regulations that apply to the public agencies themselves, such as the Public Sector (Governance) Act and the Government Instruction Manual on IT Management.

B. Network Service Providers

Section 26 of the Electronic Transactions Act ("ETA") exempt network service providers from the obligations under the PDPA, provided that sole basis for liability of the network service provider rests on the fact that the network service provider is providing (technical) access to electronic records that were created or stored by third parties over whom the network service provider has no control.

The purpose of Section of the ETA is to shield from litigation the Internet service providers and contest hosting companies (including companies that host content on the cloud) that only provide "necessary technical means" to store and access personal data.

Where however, the technology company provides, for instance, data collation and processing services, it would cease to be merely providing technical means for storage and access. It could fall within a special class of organisations known as "data intermediaries", who are nonetheless largely exempted from the key obligations under the PDPA.

C. Data Intermediaries

A data intermediary is an "organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation."

Data intermediaries are exempt from Parts 3, 4, 5, 6 (except sections 24 and 25), 6A (except sections 26C(3)(a) and 26E) and 6B as long as those data intermediaries are processing personal data on behalf of and for the purposes of another organisation **pursuant to a contract which is evidenced or made in writing**. Where the data

---

[3] Id at para. 6.10.
[4] Id at para. 6.12
[5] Id at para. 6.14.

intermediary is processing data based on oral contracts or a tacit understanding, with no evidence of a contractual relationship, the data intermediaries will be collecting information for its own benefit and will be subject to all the restrictions of the PDPA. Why do you think this is the case?

Read Daniel Seng, Chapter Four: Data Intermediaries and Data Breaches, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (2014), 80-108 [SSRN] to get a sense as to the different types of data intermediaries that are involved in daily business.

Questions:

1. What are the obligations of the data intermediaries under the PDPA?

2. Why do they receive special treatment? Is this to create an "outsourcing exemption" for Singapore data intermediaries? Is this treatment justified?

Take note that the fact that an organisation uses an intermediary to process data on its behalf does not absolve the organisation from its data protection obligations. See Section 4(3) which states, "*An organisation has the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself*."

III. PRINCIPLES OF DATA PROTECTION UNDER THE PDPA

The basic obligation of the PDPA can be summed up with reference to the two basic principles of data protection: informed consent and delimited purpose. "[A]n organisation shall not ... collect, use or disclose personal data about an individual"[6] unless the individual has given consent,[7] and an individual only gives consent where she has been notified of the purpose for which the personal data is to be collected, used or disclosed and provided consent for that purpose.[8] Any such consent given may be withdrawn by the individual "on giving reasonable notice ... at any time."[9]

Any collection, use or disclosure of personal data will be subject to the following additional principles of data protection (compare with the OECD principles from last week's reading):

- the individual has a right of **access** to personal data;[10]
- the individual has a right to **correct** her personal data;[11]
- the organisation has to ensure that the personal data collected is **accurate and complete**;[12]
- the organisation has to **protect** the personal data from unauthorized access and similar risks;[13]
- the organisation shall **cease to retain** the personal data if its purpose is no longer being served;[14] and

[6] PDPA, Section 13 (Consent required).
[7] Id.
[8] Id. at Section 14 (Provision of consent) and 20 (Notification of purpose).
[9] Id. at Section 16 (Withdrawal of consent).
[10] Id. at Section 21 (Access to personal data).
[11] Id. at Section 22 (Correction of personal data).
[12] Id. at Section 23 (Accuracy of personal data).
[13] Id. at Section 24 (Protection of personal data).
[14] Id. at Section 25 (Retention of personal data).

- the organisation shall not **transfer the personal data outside Singapore** except in accordance with prescribed requirements.[15]

A. "Reasonable" Standards for Compliance

Compliance with the PDPA is a formidable task, especially when considering that the PDPA applies to **all** organisations, not just large multinational corporations. How do we ensure that small provision stores, hawkers and poorly-resourced non-profit organisations comply with the PDPA? Is it reasonable to expect them to be able to do so?

Recognising that compliance with the PDPA will be a challenge, the PDPA adopted the standards outlined in Section 11 to determine whether or not an organisation will be found to be in breach of the PDPA. Critically, Section 11(1) states that the standard to be used to determine if a data organisation is compliant to the PDPA will be determined based on a reasonableness standard.

In other words, an organisation meets and discharges its obligation based on an "what a reasonable person would consider appropriate in the circumstances." This is ab objective assessment that will be used to determine whether each of the principles have been carried out/observed in practice.

Questions:

1. Can an organisation claim that it can be absolved for being unable to discharge certain PDPA obligations because of certain limitations of the company such as shortage of manpower and unavailability of resources?

2. How would a court assess if the obligations of a company are discharged in a "reasonable" manner?

B. Compliance Officer and Employees' Training

The imposition of an objective standard for the organisation will require the organisation to invest resources to ensure that it complies with the PDPA. This starts by requiring the organisation to designate of one or more individuals as Compliance Officers or Data Protection Officers who shall "be responsible for ensuring that the organisation complies with this Act".[16] The business contact of at least one of these officers shall be made publicly available.[17] However the PDPA obligations of the organisation still remain with the organisation, and the designation of these officers will not relieve the organisation of these obligations.[18]

C. Policies and Practices

In her role as the Data Compliance or Data Protection Officer, the officer shall require the organisation to reconfigure its existing business operations (and develop new policies and practices) to achieve compliance with the PDPA.[19] This includes developing a process to receive and respond to complaints.[20] The organisation has to actively education, train and engage the organisation's employees and communicate these new policies and

[15] Id. at Section 26 (Transfer of personal data outside Singapore).
[16] Id. at Section 11 (Compliance with act).
[17] Id.
[18] Id.
[19] Id. at Section 12(a).
[20] Id. at Section 12(b).

practices to them.[21] Information about these policies and practices have to be made available, to not just employees but also to members of the public, on request.[22]

Because there are costs associated with complying with the PDPA, and because of the move towards accountability and transparency in handling data protection policies, practices and complaints, it is recommended that the following overarching steps be taken as part of this process to develop and implement PDPA policies and practices:

- conducting an inventory map to determine what personal data is held
- aligning the IT system or infrastructure to the PDPA obligations
- conducting an on-site audit of the organisation, which will include an audit of the organisation's information security systems to ensure (continued) compliance

IV. DATA PROTECTION OBLIGATIONS

As the first of the data protection principles, the PDPA starts off by requiring an organisation to secure the consent of the individual before any personal data of that individual can be collected, used or disclosed.[23]

Consent that is given by the individual has to be "informed". That is to say that the individual must be told about the purpose behind the collection, use and/or proposed disclosure of the individual's personal data on or before the collection event. [24] Furthermore, the mechanism used to collect that data for that purpose cannot be coercive, and cannot be misguided (i.e., cannot use manipulation or tricks to receive that information).[25] The best way to appreciate the types of behaviour that is meant to be prohibited under the PDPA is to think of personal data as money. When we trick people into giving us money, we are engaging in fraud. When we coerce people into giving us money, we are engaging in extortion. That same lens should be used in analysing personal data. Where consent has to be explicitly obtained, this is described as "opt-in" consent.

Obtaining explicit consent from individuals is not always possible. Think of our daily interactions with retailers where we frequently transact and disclose our personal data. For daily activities, it is simply not practical to require businesses to obtain active consent from its customers. As a result, the PDPA includes provisions that allow businesses to collect data without the explicit written or verbal consent of the individuals. These provisions are the deemed consent provisions in Sections 15 and 15A. The PDPA also sets out situations that are exempted from the consent requirement in the First and Second Schedules.

A. Deemed Consent

Although securing the "consent" of the data protection subject or individual is a data protection principle, the implementation of this principle has been severely watered down in the PDPA, presumably in response to pressures from industries. In particular, in numerous situations, consent is "deemed" such that no express consent need be given.

---

[21] Id. at Section 12(c).
[22] Id. at Section 12(d). See also Advisory Guidelines, para. 21.13.
[23] Id. at Section 13.
[24] Id. at Section 20.
[25] Id. at Section 14.

Sections 15 and 15A of the PDPA provide for different forms of deemed consent, namely (a) deemed consent by conduct; (b) deemed consent by contractual necessity; and (c) deemed consent by notification.

Question:
Why is it necessary to have so many different situations of deemed consent?

1. Deemed consent by conduct

Deemed consent by conduct applies to situations where the individual voluntarily provides his personal data to the organisation. Think of your Starbucks barista.

The purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances. Under section 15(1), consent is deemed to have been given by the individual's act of providing his personal data. If Starbucks is calling out your actual name, without a deemed consent regime, Starbucks would have to get your consent to call your name.

Think of when Starbucks is collecting your credit card to pay for the cup of coffee. Without a deemed consent clause, Starbucks would need to obtain your consent to collect, use and disclose your credit card number and related personal data to process the payment transaction.

Let's assume that you decided to call the taxi hotline to book a taxi. You provide your home phone number, your name and your address. What can the taxi hotline operator use your data to do under the deemed consent framework? What can't the taxi hotline operator use your data to do?

Is "deemed consent by conduct" different than "deemed consent by contractual necessity"? How so? See below.

See also Re German European School Singapore [2019] SGPDPC 8 for another example of consent by conduct.

2. Deemed consent by contractual necessity

These days, we enter into contracts everywhere. In fact, every time we buy something, we enter into a contract that is governed by the Sales of Goods Act (Cap. 393). Companies also outsource their non-core activities to many contractors. A typical company may outsource to a technology vendor the activity of preparing and mailing out invoices. It outsources the activity of conducting credit card fraud checks to fraud monitoring services. It outsources payment collections to payment gateways and payment network service providers.

Therefore, when an individual provides her personal data to one organisation ("A") for the purpose of a transaction, if A has to disclose the personal data to another organisation ("B") to conduct the activities **necessary to the conclusion or performance of the contract** between A and the individual, there must be a mechanism to allow A to disclose the information to B, and from B to C (another downstream organisation) as long as the disclosure (and collection) **is reasonably necessary to fulfil the contract** between the individual and A. Otherwise, it would be necessary for A to obtain explicit consent from the individual to disclose that individual's personal data to B, C, and all downstream organisations.

Contrast Section 15(3) of the PDPA to the situation in Korea where the Personal Information Protection Act requires all data collectors to disclose all the first level downstream organisations to which an organisation discloses data.

Question:

Can you imagine a situation where a company could run afoul of the deemed consent rule? In other words, let's assume a company is entitled to collect information under the deemed consent rule. How could the company's further collection/use/disclosure breach the PDPA?

3. Deemed consent by notification

Remember when we said that Section 14 of the PDPA restricts the collection of data through coercion or trickery? For example, we had discussed that sending a marketing email message to customers and requiring them to return a mailer to actively opt out of future marketing messages is not considered to be a valid mechanism for obtaining consent.

Let's consider Section 15A of the PDPA.

Section 15A of the PDPA allows a company to notify an individual of the organisation's intent to collect, use or disclose personal data for a purpose and take the customer's silence (i.e., customer's failure to actively opt out of the collection, use or disclosure) as deemed consent to the collection, use or disclosure of that individual's data.

In its Advisory Guideline, para. 12.23, the PDPC stated that: "[d]eemed consent by notification is useful where the organisation wishes to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had originally collected the personal data for, and it is unable to rely on any of the exceptions to consent (e.g., business improvement, research) for the intended secondary use." Although this seems to fly in the face of the Section 14 restrictions, Section 15A mandates an organisation to actively undertake its own risk assessments, that must be documented, to justify why reliance on Section 15A is allowed.[26] The PDPC recognises that the Section 15A deemed consent rule could be abused by organisations when it comes to marketing materials (i.e., spam). Therefore, Section 15A(3) specifically states that the deemed consent rule "*does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose*."

The PDPC's Advisory Guidelines on Key Concepts in the PDPA (Revised 1 October 2021) provides the following example of obtaining consent by providing appropriate notification to users of mobile application

A health app company provides a mobile application that collects, uses and discloses personal data relating to individuals' lifestyle and wellness (e.g. number of steps walked, height, weight, age and gender). Users are able to view their activity data (e.g. sleep patterns, periods of activity, number of calories lost) through the mobile application.

[26] Advisory Guidelines, para. 12.23-12.26 for the documentation required to ensure Section 15A compliance under the deemed consent by notification rule. As the IS professional, you need to make sure that someone in your organisation archives the evidence for production to the PDPC when required if your organisation decides to collect / use / disclose personal data under the exception provided in Section 15A.

The health app company intends to use the lifestyle and wellness data collected from its users to provide a personalised weight loss programme for its users. It intends to use the users' personal data to provide the personalised programme through the application installed on their devices. It assesses that there is no likely adverse effect to users in using their personal data for this purpose. Thereafter, each user can decide whether to participate after viewing the personalised programme (in which case express consent will be obtained).

Question:

Why do you think the business chose to rely on deemed consent by notification? Why can't the business rely on the business improvement or research exception?

4. Exceptions to the consent obligation

The PDPA was most recently amended in February 2021. Before that amendment, the PDPA set out the circumstances under which consent could be inferred to have been given, and these circumstances were spread out over three schedules – the Second Schedule, Third Schedule and Fourth Schedule. With the February 2021 amendment, all of the items allowing for the collection, use and disclosure of personal data under an implied consent have been consolidated under the First and Second Schedules.

Review the First and Second Schedules to understand the exceptional circumstances where personal data may be collected, used and disclosed without the need for consent.

Questions:

1. How are the items in the First and Second Schedules similar or different?

2. How do these situations fit with the principle of consent as set out in Part 4 of the PDPA? What about the OECD Collection Limitation Principle and Use Limitation Principle?

5. Withdrawal of consent

Of course, with the goal of giving control back to individuals over their personal data, there must be a mechanism for individuals to withdraw the consent that they have given for the use, collection and disclosure of their data. But if an individual has the right to withdraw consent, a withdrawal of that consent could have severe impact on organisations.

Some questions you should consider in light of the individual's right to withdraw consent:

- Do you know where the data is stored?
- What about data that is stored in e-mail accounts?
- What about data stored on local drives?
- How does your organisation manage and govern the data? Do you know how the data is flowing throughout the organisation?
- How can you make sure that upon withdrawal of consent, that your organisation can effectively comply with the PDPA?

The PDPA is silent as to whether an individual may provide reasonable notice to withdraw her "implied consent" given for collection, usage and disclosure activities which

were sanctioned under the First and Second Schedules. However, Section 16(4) of the PDPA states that in the event an individual withdraws her consent, the organisation is to "*cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual* ***is required or authorised*** *under this Act or other written law*." Since the PDPA allows the collection of information without consent under the First and Second Schedules, presumably, a withdrawal of implied consent would not be possible.

Withdrawal of consent is separate from the requirement to delete the data. The PDPA does not require an organisation to delete or destroy the individual's personal data upon request. Contrast this with the GDPR which does provide individuals the right to demand the deletion or destruction of their personal data. Under the PDPA, organisations may retain personal data in their documents and records in accordance with the Care of Personal Data provisions in Section 25 of the PDPA.

B. Purpose Limitation

1. General

A cardinal data protection principle is that personal data of the individual may only be used for those purposes which are "reasonably appropriate" and for which the individual has been informed. See Sections 18 and 20 of the PDPA.

However, the First and Second Schedule provide clear instances where the individual need not be informed about the purpose for which the data is collected, used or disclosed.

2. Employees

Employees are a special class of individual data subjects singled out for treatment by data organisations. In particular, as they have very close working relationships with their employer organisations, the collection, use and disclosure of their personal data may be an incident of, and a necessary part of, employment.

Paragraphs 2, 3, 9 and 10 of Part 3 of the First Schedule and Part 4 of the First Schedule specifically allow employers to retain the personal data of their employees in connection with their employment, for evaluative purposes, for investigations, and for business asset transactions.

However, it is noteworthy that notwithstanding that Section 17 of the PDPA and the First Schedule frees an employer to use, collect and disclose employee personal data without the individual employee's consent, where the data is collected, used or disclosed for the purpose of entering into an employment relationship or managing or terminating that employment relationship, Section 20(4) requires the organisation to disclose this purpose "on or before" such data is collected used or disclosed.

As information security professionals, you will be assisting the human resource ("HR") department with setting up technology platforms for handling a lot of employee related information. Moreover, many HR operations are outsourced these days and more and more HR technology (e.g., technology for profiling of employees) are being employed, frequently at very cheap prices. When assisting the HR department with selecting the right set of technologies to use to perform critical HR functions, you should be sensitive to the requirements of the PDPA and ensure that you select vendors that can comply with the

terms of the PDPA as any non-compliance by the vendors, will be your organisation's responsibility.

See https://www.lexology.com/library/detail.aspx?g=4c9e6e94-5fad-4b66-afc3-db447e61c78a. See also Lim YF, Chapter Eight: Data Protection in the Employment Setting, Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World (2014).

C. Access Rights

One of the most important data protection principles is that of guaranteeing the individual as the data subject a right of access to her own personal data, as well as the ways in which her personal data may have been used or disclosed. The PDPA places limits on this access. See Section 21 and the Fifth Schedule.

Questions:

1. What does this principle (and the ensuing exceptions) entail as regards the way in which personal data is to be collected by the data organisation?

2. Can you list the types of meta-data that have to be collected for a piece of personal data?

D. Correction Rights

The corollary to the individual's data access rights is her right to correct her personal data. See Section 22. See exceptions to these rights in the Sixth Schedule.

Questions:

1. Why should an individual be given the right to correct her personal data? What advantages does it have for an individual?

2. How would the individual exercise her right in practice? What operational and IS issues would there be?

E. Accuracy, Protection and Retention

As a consequence, a data organisation also has rights to safeguard the personal data. Safeguarding the data also includes an obligation not to retain the data when the purpose for which the data is collected is spent. See Sections 23, 24 and 25.

A brief discussion of the technical and operational schemes that an organisation will put in place to ensure that the data protection principles of accuracy, protection and retention are observed can be found in the following reading:

Tan, Bryan, Chapter Six: *A Practitioner's Perspective, Data Protection Law in Singapore: Privacy and Sovereignty in An Interconnected World* (2018), para. 6.13-6.42.

Questions:

1. What (legal, technical and operational) schemes would an organization put in place to ensure that personal data that it collects is (a) accurate, and (b) protected from unauthorized access, collection and use, and that it ceases to retain such personal data as soon as the purpose for which it was collected was no longer necessary? How would you deal with the following scenarios under the PDPA:

- inadequately documented personal data (e.g. source, nature of data, purpose, currency etc.)
- poor (physical and electronic) document management
- unmonitored outgoing business email communications
- weak or non-existent information security implementations for hardware
- use of in-house or third-party software tools for managing personal data
- social engineering attacks

2. What other (countervailing) factors ought to be considered when implementing these schemes?

Read Singapore Health Services [2019] SGPDPC 3 (14 January 2019) as we will go through the case in class.

See also, Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database (10 January 2019).

F. Notification of Data Breaches

With the latest amendments that were promulgated in February 2021, organisations must provide breach notifications if a breach "(a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale." The PDPC engaged in a consultation period with businesses over a course of 2 years before proposing this section to be included into the amendment to the PDPC. The purpose of adopting this requirement is, as discussed in the Second Reading of the Personal Data Protection (Amendment) Bill:

"*To further strengthen organisations' accountability, clause 13 introduces a system for mandatory notification to the Personal Data Protection Commission, or PDPC, when a data breach occurs*."

Under this Clause, organisations must notify the PDPC of data breaches that are of significant scale. In addition, organisations must notify both the PDPC and affected individuals when data breaches result, or are likely to result, in significant harm to individuals. This places the onus on organisations to assess the scale and impact of data breaches, ensures they are duly accountable to individuals for the personal data in their care, and empowers individuals to take timely measures to protect themselves if a data breach occurs."

As explained in the parliamentary debates, new sections 26A-D place the onus the organisations to conduct their own risk assessment to determine if breaches should be notified. When required, the organisation is required to notify the breach not only to the individuals whose data have been breached, but also to the commission.

Questions:

1. Can you give an example of a breach that would not be required to be notified?

2. If a retailer suffers a breach of 300 sets of customer data that include the customers' name, shipping addresses and email addresses, would this be a notifiable breach?

3. What if instead of 300 sets of data, we increase that number to 500?

See the Advisory Guidelines Section 20.

The purpose of introducing a data breach notification regime was to shift the focus of personal data protection towards an accountability approach in line with international trends and best practices in data protection laws. However, with the introduction of an accountability approach, it places a lot of the onus of risk assessment on the organisation.

Questions:

1. As an IS professional, in which situations do you think you will encounter the most difficulty with this accountability-based approach?

G. Obligations of Data Intermediaries

The obligations of data intermediaries are set out in Section 4(2) of the PDPA. Do you know what they are? What happens if there is no written contract between the data intermediary and the data organisation?

See Seng, Daniel, *Chapter Seven: Data Intermediaries and Data Breaches, Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (2nd ed).

See Personal Data Protection Digests: [2020] PDP Digest [LINK] to get a better understanding of the obligations of data intermediaries and how their actions will impact the liabilities of the data organisations.

H. Transfer of Data Overseas

The issue of the transfer of personal data overseas can be a very important one, especially where Singapore seeks to position itself as the IT hub for the region. In particular, the use of technologies like cloud computing make the import and export of personal data across geographical borders feasible and occasionally transparent to data organizations and data intermediaries. This can be a problem for jurisdictions like the EU, which exercise strict data protection controls over the personal data of its citizenry. Transborder data flows into a jurisdiction with weaker data protection laws that do not meet EU criteria will trigger sanctions against and lead to a termination of future data flows to the targeted jurisdiction. The EU traditionally takes the position that US laws do not provide adequate safeguards to the protection of personal data. As a result, data transfers between these two jurisdictions had to rely on frameworks for regulating transatlantic data exchanges. These two frameworks, the Safe Harbor and the Privacy Shield, have both been declared invalid by the European Court of Justice. As a result, data transfers between these two jurisdictions now need to rely on contracts that include standard contractual clauses that have been approved by the EU.

Section 26 regulates data flows across border. For data transfers between Singapore and non-Singapore countries, generally, the best practice is to ensure that there are contracts in place regulating cross-border transfer flows. Be aware that these contracts will need to include contracts between parent and subsidiary entities because legally speaking, these are two different entities and a cross border data transfer between subsidiary and parent companies that are conducted without contractual safeguards will likely run afoul of the PDPA.

Data transfers to organisations that have been certified under certain programs will be deemed compliant under the PDPA. These programs include: Asia Pacific Economic Cooperation Cross Border Privacy Rules ("APEC CBPR") System, and the Asia Pacific

Economic Cooperation Privacy Recognition for Processors ("APEC PRP") System. See the Advisory Guidelines Section 19.

I. Data Portability (not applicable in this class)

The Personal Data Protection (Amendment) Bill also included the concept of data portability. This is not yet in effect as the regulations are still being drafted, but I have mentioned its existence for completeness. For more information, see clause 13 of the Personal Data Protection (Amendment) Bill.

V. CRIMINAL SANCTIONS

The February 2021 amendments introduced more criminal provisions into the PDPA. Specifically, Part 9B sets out new offences for (a) the unauthorised disclosure of personal data, (b) the improper use of personal data that results in personal gain for the offender or another person, or harm or loss to another person; and (c) the unauthorised re-identification of anonymised information. Changes to related laws were made to align the public and private sector data regimes.

During the parliamentary debates, at the Second Reading, Minister Iswaran stated that: "[w]hile the primary responsibility and liability for breaches of the PDPA rest with organisations, these new offences are aimed at individuals who know that their actions are not authorised or who act recklessly. The clause provides for defences to the new offences, such as independent testing of anonymisation deployed in information security systems. Also, these offences should not apply in situations where the conduct is solely in the nature of a private dispute, which should continue to be resolved through civil suits or other forms of dispute resolution."

Question:

In your opinion, how do these new provisions enhance/detract from the Computer Misuse Act? What type of offences do they address that is not already addressed in the CMA?

VI. ENFORCEMENT

A. Mechanism for Enforcement

The PDPA provides remedies for an aggrieved individual seeking redress against the data organisation. The individual can apply to the PDPC to review an organisation's decision. The PDPC can give directions to the data organisation,[27] or it could, with the consent of the individual complainant, refer the matter to mediation.[28]

The PDPA also provides a private right of action by a person who suffers loss or damage directly as a result of a breach of the provisions in Part 4, 5, 6, 6A or 6B or by a person of any provision of Division 3 of Part 9 or 9A. See Section 48O.

Questions:

1. Under what circumstances would an individual pursue his remedies against an organization in a right of private action? What is intended by the requirement that a

[27] Section 48H.
[28] Section 48G.

Commission has to render a final decision before a right of private action may accrue?

2. How viable is this option for aggrieved individuals as data subjects in practice?

The PDPC may also, on its own volition, commence an investigation. See Section 50.

B. Financial Penalties

The maximum financial penalty for breaches of Parts 3 to 6, and the new Parts 6A and 6B (data portability, which is not yet enacted) will be up to $1 million. In due course, this amount will be increased to 10% of an organisation's annual turnover in Singapore or $1 million, whichever is higher. See Advisory Guidelines, para. 21.14(e).

VII. DO NOT CALL

A substantial part of the PDPA is taken up by provisions that deal with the setting up of the Do Not Call Registry, a system to ensure that unsolicited telephone calls are not made to registered telephone numbers, and recent changes to rationalise and harmonise the requirements across all modern digital channels for direct commercial communication with consumers.

We will not discuss these provisions for this module.