LEGAL ASPECTS OF INFORMATION SECURITY IFS4101

WEEK 12, WELLY TANTONO, DIS, SOC, NUS

PERSONAL DATA PROTECTION ACT (CON'T)

DATA BREACH NOTIFICATION

- All data protection regulators have been clear that accountability is part of the requirements of compliance with data protection laws. To that end, many data protection laws worldwide require organisations to report data breaches to the (a) regulators and/or (b) data subjects.
- **Section 26B** of the PDPA states that breach notification is required when the breach:
  - results in, or is likely to result in, significant harm to an affected individual; or
  - is, or is likely to be, of a significant scale

DATA BREACH NOTIFICATION

- **Section 26C** of the PDPA 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 PDPC. However, there are circumstances under which only the PDPC needs to be notified but not the individuals. Generally, assessments must be completed within 30 days (see Advisory Guidelines Paragraph 20.4).
- Breach notification obligations apply to both **organisations** and **data intermediaries**. Data intermediaries must notify their organisation.
- Organisations (other than public agencies) must carry out a risk assessment to determine if the data breach reported by the data intermediary is a notifiable data breach. The data intermediary **has no obligation to conduct risk assessment**.

DATA BREACH NOTIFICATION

- What is the definition of "significant scale"?
- Section 26B(3) of the PDPA states that a data breach is of a significant scale "if the data breach affects not fewer than the prescribed number of affected individuals" or in other prescribed circumstances.
- The prescribed number of individuals is stated in paragraph 20.20 of the Advisory Guidelines:
  - "*Data breaches that meet the criteria of significant scale are those that involve the personal data of 500 or more individuals. Where a data breach affects 500 or more individuals, the organisation is required to notify the Commission, even if the data breach does not involve any prescribed personal data in paragraph 20.15.*"
- Note that the 500 number is tied to **individuals**…. not data sets.

DATA BREACH NOTIFICATION

- If it is not possible to tell how many individuals a data breach affects (e.g., users may have created multiple accounts), the organisation can estimate and decide whether to be conservative and overcount and inform the PDPC or to be aggressive and undercount. The risk with undercounting is when the organisation discovers that it actually needs to notify the PDPC, and notifies the PDPC late, there is a risk of fines. Organisations will need to balance the risk of fines and reputational harm against not wanting to alert the PDPC.
- Organisations can take the conservative approach and overcount and notify the PDPC, but wait until it has determined the actual number of affected individuals to determine whether or not notification to affected individuals are required.

SIGNIFICANT HARM

- What is the definition of "significant harm"?
- Section 26B(2) of the PDPC states that a breach results in significant harm "if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual" or in other prescribed circumstances.
- Paragraph 20.15 of the Advisory Guidelines defines "prescribed personal data" to include:
  - **full** name or alias or **full** national identification number **in combination with** items in sub-paragraphs (i) to (xxv) of Paragraph 20.15. Note that the full name/alias/national identification number standing alone, don't quite make it to that level of concern requiring immediate notification.
    - **Why do you think this is the case?**
  - **personal data relating to an individual's account (both active and dormant)** with an organisation, including account identifiers and access credentials (e.g., password/security code/access code/response to security question/biometric data, etc. used to allow access to or use of account)
- **EXCLUDES** personal data that is publicly available and any personal data that is disclosed under any written law[7] (e.g., pay information issued by employers under the Employment Act).

SIGNIFICANT HARM

- Sub-paragraphs 20.15(i) to (xiii) relate to financial information that is not usually publicly disclosed
- Sub-paragraph 20.15(xiv) to (xvii) relate to information that identify vulnerable persons such as those under protective orders from abusive spouses or young offenders
- Sub-paragraph 20.15(xviii) insurance policy information that is not public
- Sub-paragraphs 20.15(xiv) to (xxiii) relate to specific medical information
- Sub-paragraph 20.15(xxiv) relate to information concerning adoption
- Sub-paragraphs 20.15(xxv) relate to private key used to create a secure electronic record, verify the integrity of a secure electronic record or verify the authenticity or integrity of a secure electronic signature.

FORM OF NOTIFICATION

- Advisory Guidelines Paragraphs 20.38 and 20.44 set out the content that must be included in breach notifications

BREACHES THAT HAPPEN OVER TIME

- Different categories of personal data may be lost or compromised at different times. The organisation **must notify the Commission and/or affected individuals** if the assessment reveals that the breaches are likely to be linked (e.g., same perpetrator or same technique used or circumstances such as discovery of a combined database containing both sets of data discovered online)

EXCEPTIONS TO NOTIFICATION

- Breaches that happen **within an organisation** is not a notifiable data breach. E.g., someone within the HR department sends an email attachment containing personal data to another department within the same organisation that is not authorized to receive such information.
- Notification to the affected individuals (affected data subjects) can be avoided if the conditions of Section 26D(5) (known as the remedial action exceptions) are in place:
  - on or after assessing that the data breach is a notifiable breach, the organisation takes any action that **renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or**
  - the organisation had implemented, prior to the notifiable data breach event, any technological measure that renders it unlikely that the notifiable breach will result in significant harm to the affected individual
- Remedial actions can be taken after notifying the PDPC.
- All exceptions can be overridden by law enforcement agencies or the PDPC. Section 26(D)(6).

NOTIFICATION DOES NOT IMPUTE LIABILITY

- To encourage notification, Section 26D(8) states that notification of the PDPC or an affected individual cannot be treated to mean that the notifier has breached its duty or obligation under any written law or rule of law, or any contract, as to the secrecy or other restriction on the disclosure of information, or any rule of professional conduct.

DATA BREACH NOTIFICATION

- *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?*
- *What if the number of customers involved exceed 500?*

TIMEFRAMES FOR NOTIFICATION

- As soon as **practicable** but not exceeding **3 calendar days** from the day the organisation **determines there is a notifiable breach**. In other words, can be more than 3 calendar days from when the actual incident occurred.

CRIMINAL SANCTIONS FOR UNAUTHORISED DISCLOSURE

- Sections 48D and 48E of the PDPA makes it a crime for the unauthorised disclosure / use, respectively, of personal data where the discloser:
  - **Knew** that the disclosure was unauthorized or
  - **Was reckless** in making that disclosure
- Defence available if any of the following can be proven on **a balance of probabilities** (i.e., more than 50%; this is not a beyond reasonable doubt standard):
  - Personal data that was disclosed was, at the time of the disclosure, publicly available; and where the personal data was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case;
  - Disclosure was (a) permitted or required by or under the law; (b) required by court order; (c) not reckless (i.e., was reasonable about the accused having the right to disclose); or (d) in any other circumstances, or for any other purpose, prescribed.

ENFORCEMENT

- How does an individual pursue his remedies for breach of the PDPA against an organisation?
  - application to PDPC to review organisation's decision: PDPA Section 48H
  - PDPC initiates its own investigation: PDPA Section 50
  - individual sues organisation for loss or damage: PDPA Section 48O

BREAK

CASE STUDY : IMPROPER HANDLING OF PERSONAL INFORMATION OF BLOOD DONORS BY HEALTH SCIENCES AUTHORITY

- The Health Sciences Authority (HSA) was alerted on 13 March 2019 that one of its vendor's servers contained a HSA database that was not adequately safeguarded against access over the internet. The vendor was Secur Solutions Group Pte Ltd (SSG). SSG provided services to HSA and was working on a database containing registration-related information of 808,201 blood donors: Name, NRIC, gender, number of blood donations, dates of the last three blood donations, and in some cases, blood type, height and weight. The database contained no other sensitive, medical or contact information.
- A cybersecurity expert had discovered this vulnerability and alerted the Personal Data Protection Commission. … The expert has confirmed to HSA that he does not intend to disclose the contents of the database. HSA is in contact with the expert on deleting the information. … Preliminary findings from HAS's review of the database logs show that other than the cybersecurity expert who raised the alert, no other unauthorised person had accessed the database.
- HSA had provided the data to SSG for updating and testing. SSG placed the information in an internet-facing server on 4 Jan 2019 and failed to institute adequate safeguards to prevent unauthorised access. It had done so without HSA's knowledge and approval, and against its contractual obligations with HSA.

CASE STUDY : IMPROPER HANDLING OF PERSONAL INFORMATION OF BLOOD DONORS BY HEALTH SCIENCES AUTHORITY

- Question: Was there a potential issue under the Computer Misuse Act?
- "*We will not be taking any legal action against him because he had reported the vulnerability to us straightaway, and had no intention to keep, use or expose the contents of the database, and has not done so*," said the Senior Minister of State (for Health Edwin Tong).

MCI'S RESPONSE TO PQS ON HSA DATA LEAK AND PUBLIC SECTOR DATA BREACHES (1 APRIL 2019)

- ***2747. Ms Sylvia Lim:** Regarding the recent data leak of more than 800,000 blood donors' personal information from the database of HSA (a) what is the role of the Personal Data Protection Commission in investigating this incident; (b) whether any review is being done to ascertain whether HSA has acted reasonably in protecting the personal data including whether the contractual obligations between HSA and its IT vendor reasonably safeguarded the personal information entrusted to these parties.
- ***2734. Ms Irene Quay Siew Ching:** In view of data breaches across public IT systems (a) whether it is justifiable for public agencies to be exempted from Personal Data Protection Act; (b) what recourse do citizens have, other than to complain to agencies or seek civil action; and (c) whether there should be a tangible penalty meted out to these public agencies for public accountability.

MCI'S RESPONSE TO PQS ON HSA DATA LEAK AND PUBLIC SECTOR DATA BREACHES (1 APRIL 2019)

1. What is the role of the PDPC (where public sector is involved)
2. Whether HSA had acted reasonably in protecting the personal data

- Personal Data Protection Commission (**PDPC**) is investigating Secur Solutions Group Pte Ltd, which is a private company and vendor of IT services to HSA. If found to be in breach of the Personal Data Protection Act (**PDPA**), PDPC will take the appropriate enforcement actions against the company, such as issuing directions and imposing financial penalties.
- The Senior Minister of State for Health has earlier outlined the review of HSA's data security policies and practices that is being undertaken. As HSA is a Government agency, the **Smart Nation and Digital Government Group** is also conducting an investigation into the incident.

MCI'S RESPONSE TO PQS ON HSA DATA LEAK AND PUBLIC SECTOR DATA BREACHES (1 APRIL 2019)

1. Whether it is justifiable for public agencies to be exempted from Personal Data Protection Act

- Implicit in the Member's question is the presumption that public sector agencies are not accountable for their data protection practices or not held to a high standard because the PDPA does not apply to them. That is wrong and simply not the case. Public sector agencies are subject to a different piece of legislation and other regulations. In particular, public sector agencies have to comply with the Government Instruction Manuals and the Public Sector (Governance) Act (**PSGA**). Collectively, they have comparable if not higher standards of data protection compared to the PDPA, and similar investigations and enforcement actions are taken against data security breaches.

- PDPA does not apply to public agencies because there are fundamental differences in how the public sector operates, which requires a different approach to personal data protection compared to the private sector. In order to enable a whole-of-government approach to the delivery of public services, personal data has to be managed as a common resource within the public sector. The considerations are different in the private sector, as there is no such expectation of a holistic approach to the delivery of commercial services across private organisations.

MCI'S RESPONSE TO PQS ON HSA DATA LEAK AND PUBLIC SECTOR DATA BREACHES (1 APRIL 2019)

2. What recourse do citizens have, other than to complain to agencies or seek civil action?
3. Whether there should be a tangible penalty meted out to these public agencies for public accountability?

- Citizens have the same recourse for a data breach in the public sector as with the PDPA. Where citizens suspect that their data has been mishandled by a private sector organisation, they can lodge a complaint with the PDPC; or with GovTech, if a public sector agency is involved. In practice, there are no wrong doors and the complaint will be directed to the relevant agencies for follow-up. Affected individuals can also seek mediation or take civil action against the organisation or agency which mishandled the data.
- Public officers who flout the Government's data security rules, and are found to have misused or disclosed data in an unauthorised manner, could be held criminally liable under the PSGA. The penalties include fines of up to $5,000 or a jail term of up to two years, or both. **It is not meaningful to impose financial penalties on public sector agencies because the cost of such penalties would ultimately have to be borne by the same public purse**.
- Convened Public Sector Data Security Review Committee that produced a report in November 2019.

CONCLUSIONS OF THE PUBLIC SECTOR DATA SECURITY REVIEW COMMITTEE REPORT

Desired Outcomes	Key Recommendations
Protects data and **prevents** data compromises	1. Enhance technology and processes to effectively protect data against security threats and prevent data compromises.
Detects and responds to data incidents	2. Strengthen processes to detect and respond to data incidents swiftly and effectively.
Competent public officers embodying a **culture of excellence**	3. Improve culture of excellence around sharing and using data securely, and raise public officers' competencies in safeguarding data
Accountability for data protection at every level	4. Enhance frameworks and processes to improve the accountability and transparency of the public sector data security regime
Sustainable and resilient manner	5. Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime that can meet future needs.

KEY RECOMMENDATION 1: ENHANCE TECHNOLOGY AND PROCESSES TO EFFECTIVELY PROTECT DATA AGAINST SECURITY THREATS AND PREVENT DATA COMPROMISES

- The Committee proposed 13 technical and 10 process safeguards, ultimately to:
  - Reduce the surface area of attack by **minimising** data collection, data retention, data access and data downloads.
  - **Enhance** the **logging** and monitoring of data transactions to detect high-risk or suspicious activity.
  - Protect the data directly **when** it is **stored** and **distributed** to render the data unuasable even when extracted or intercepted.
  - Develop and maintain expertise in advanced technical measures
  - **Enhance** the data security **audit framework** to detect gaps in practices and policies before they result in data incidents
  - Enhance the **third party management framework** to ensure that third parties handle Government data with the appropriate protection

KEY RECOMMENDATION 2: STRENGTHEN PROCESSES TO DETECT AND RESPOND TO DATA INCIDENTS SWIFTLY AND EFFECTIVELY

- The Committee's recommendations for managing data incidents are structured around the five stages of "Detect", "Analyse", "Respond", "Remediate" and "Post-Incident Follow-up".
- What is most interesting about Key Recommendation 2 was the call to institute a framework for all public agencies to promptly notify individuals affected by data incidents with significant impact to the individual. This notification framework is similar to the mandatory data breach notification regime in the current PDPA.

CASE STUDY: SINGHEALTH

- Let's consider the key recommendations. How would they have helped to mitigate the SingHealth type of incident?

CASE STUDIES 1 AND 2

- Break into groups and discuss the proposed answers to the questions posed in Case Studies 1 and 2 distributed before class.

IS THERE ANOTHER WAY?

"I'm speaking to you from Silicon Valley, where some of the most prominent and successful companies have built their businesses by lulling their customers into complacency about their personal information ...They're gobbling up everything they can learn about you and trying to monetize it. We think that's wrong. And it's not the kind of company that Apple wants to be.

We don't think you should ever have to trade it for a service you think is free but actually comes at a very high cost. This is especially true now that we're storing data about our health, our finances and our homes on our devices.

We believe the customer should be in control of their own information. You might like these so-called free services, but we don't think they're worth having your email, your search history and now even your family photos data mined and sold off for god knows what advertising purpose. And we think some day, customers will see this for what it is."

Tim Cook, Apple (Jun. 2, 2015)

CONCLUSIONS

- The first version of the PDPA was alright as "first try" of data protection legislation – but legislative model was not "cutting edge" and had too many business-oriented compromises
- The latest version of the PDPA attempts to correct some errors with the first version, by strengthening the accountability regime, increasing the financial penalties, and placing more obligations (e.g., breach notification) on organisations. The PDPC was also very active in its enforcement, although the bulk of its investigations were brought to it by complainants.
- However, we continue to see the tension between the data protection objectives and the need to balance against business interests. We see this with the revised deemed consent rules that gave greater certainty to businesses, legitimizing the downstream distribution and use of information, as well as implementation of rules that allow further data harvesting to create new products.

CONCLUSIONS

- Data protection laws require meta data for tracking use and disclosure of personal data
  - additional layer of cost and operational integrity (plus authentication and security)
- PDPA implementation adds additional implementation issues from IS perspective
  - differentiating between different types of data sources (to differentiate between "personal data" that fall within vs. outside the scope of the PDPA)
  - differentiating between the various exemptions that are permitted under the First and Second Schedules

CONCLUSIONS

- "Reasonableness" standard means a lot of the onus for deciding how to guide or develop and implement IS policies is placed into the hands of the organisation and the IS administrator. This means that IS professionals must step up and get comfortable with risk management
- The only "objective" benchmark in absence of coherent industry best practices is reliance on certifications (Trustmark in Singapore, and the APEC certifications)
- Always a trade-off between interests of individuals and interests of organizations
- Not easy to translate between benefits (better marketing, improved employee management) and costs (resources, expenditures, training, legal penalties, societal sanctions, loss of business) to organisation

CONCLUSIONS

- PDPA continues to be a work in progress
- MCI continues to resist upgrading PDPA to the gold standard (GDPR) because of the need to balance business interests with protecting the system to enhance consumer trust. However, pressure will likely keep building because Singapore companies that do business in EU already have to comply with GDPR. The more globalized Singapore wants its companies to become, the more Singapore will have to get its businesses ready to become GDPR ready.