Tutorial 4

Isa bin Haron, Lok Ke Wen, Ivan Chong

Part 1

1.

(5) Except where business contact information is expressly referred to, Parts III, IV, V, VI and VIA shall not apply to business contact information.

[Act 40 of 2020 wef 01/02/2021]

Part 1

2.

(4) This Act shall not apply in respect of —

(*a*) personal data about an individual that is contained in a record that has been in existence for at least 100 years; or

(*b*) personal data about a deceased individual, except that the provisions relating to the disclosure of personal data and section 24 (protection of personal data) shall apply in respect of personal data about an individual who has been dead for 10 years or fewer.

Part 1

3. The GDPR applies to organizations that **do not have any presence in the EU**, but that **offer goods, services or monitor the behavior of persons in the EU.**

Part 1

4.

The CCPA obligations apply to an organization ("**business**") that:

1. is **for-profit**;
2. collects **consumers' personal information**, or on the behalf of which such information is collected;
3. **determines the purposes and means** of the processing of consumers' personal information;
4. **does business in California**; and
5. meets any of the following thresholds:
   - has **annual gross revenue in excess of $25 million**;
   - alone or in combination, **annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices**; or
   - **derives 50% or more of its annual revenues from selling consumers' personal information.**

The CCPA also applies to any entity that controls or is controlled by the business. There are no obligations directed specifically at "**service providers**," other than using the personal information solely at the direction of the business

Question 1

- Discussion details
  - What the rights are?
  - How are the rights communicated? By whom?
  - How do consumers request the rights?
  - Can businesses ask for more information? For what purposes?
  - How long do businesses have to respond to requests?
  - Can requests be denied? For what reasons?

Question 1

California Consumer Privacy Act (CCPA)

- Right to know
  - Consumers may request business to disclose what personal information they have collected, used, shared, or sold, and the reasons for why they collected, used, shared, or sold that information. Business must provide information for 12-month preceding the request, free-of-charge.
  - Business must provide at least two methods to submit request, no account creation.
  - Must respond within 45 calendar days, with 45 day extension by notification.
  - May request more information specifically for verification purposes.
  - May deny request
- Right to delete
  - Consumers may request business to delete personal information collected and their service providers to do the same. However, service providers does not have to act on the request unless request is submitted to them directly.
  - Business must provide at least two methods to submit request, no account creation.
  - Must respond within 45 calendar days, with 45 day extension by notification.
  - May request more information specifically for verification purposes.
  - May deny request
- Right to opt-out
  - Consumers may request business to stop selling information by opting-out. Businesses must stop selling personal information immediately unless authorization to do so at a later date.
  - Business has to provide clear and visible “Do Not Sell My Personal Information” link on website or other methods stated in privacy policy to allow consumer to submit a request.
  - Not required but may be needed to ensure business stop selling the right person’s personal information.
  - May deny request if necessary for compliance, and/or personal information is exempt from CCPA.
- Right to non-discrimination
  - Businesses cannot treat consumers differently for exercising their rights under CCPA

Question 2

GDPR Key data protection principles:

- **Lawfulness, fairness and transparency:** Personal data is to be ***processed*** lawfully, fairly and in a transparent manner
- **Purpose limitation:** Personal data is ***collected for specific, explicit and legitimate purposes*** and not further processed than necessary
- **Data minimization:** Personal data collection is adequate, relevant and ***limited*** to its intended purpose
- **Accuracy:** Personal data is to be ***accurate***, updated when necessary, and erased/rectified without delay in the event of inaccuracies.
- **Storage limitation:** Personal data is to be kept ***no longer than necessary*** for the purposes it was processed.
- **Integrity and confidentiality:** Personal data is processed in a way that ensures appropriate ***security*** of personal data
- **Accountability:** The data controller is responsible for being able to demonstrate GDPR compliance

Question 3

Requirements under security of processing for GDPR:

- Taking into account the state of the art, the **costs** of implementation and the **nature**, **scope**, **context** and **purposes** of processing as well as the **risk** of varying likelihood and severity for the **rights and freedoms** of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
  - the **pseudonymisation and encryption** of personal data;
  - the ability to ensure the ongoing **confidentiality, integrity, availability** and resilience of processing systems and services;
  - the ability to **restore** the availability and access to personal data in a **timely** manner in the event of a physical or technical incident;
  - a process for **regularly testing, assessing and evaluating** the effectiveness of technical and organisational measures for ensuring the security of the processing.

Question 3

Requirements under security of processing for GDPR:

- In assessing the **appropriate level of security account shall be taken** in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
- Adherence to an approved **code of conduct** as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
- The controller and processor shall take steps to **ensure that any natural person** acting under the authority of the controller or the processor who has access to personal data **does not process** them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Question 4

GDPR

- Who is protected?
  - All living persons, not necessarily EU citizens or residents.
- Who must comply?
  - Businesses, public bodies and institutions, not-for-profit organizations in the EU. As long as serving people located in the EU. If an organization is outside the EU but processing/serving anyone in the EU, then they must comply with GDPR.
- What is the definition of personal information?
  - Any information that directly or indirectly relates to an identified or an identifiable individual.
- Data breach notification requirement
  - Controller - Shall notify about data breach to supervisory authority (agency responsible for GDPR in each country). To notify no later than 72 hours after becoming aware unless data breach is not so severe. Later notifications must be accompanied with reasons for delay.
  - Processor - Shall notify controller without any delays after becoming aware of a personal data breach.
  - Notification to supervisory authority to include specific details such as nature of breach, contact details of DPO, consequences of breach, measure taken or proposed to address the data breach
- Violation penalty scheme
  - Low severity - 2% of global annual turnover or 10 million euros, whichever is higher
  - High severity - 4% of global annual turnover or 20 million euros, whichever is higher.

Question 4

CCPA

a. Who is protected
    i. A natural person who is a California resident, including when they are out of state.
b. Who must comply
    i. Organisations that are for-profit and do business in California that meet any of the following:
        - Have a gross annual revenue of over $25 million;
        - Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices
        - Derive 50% or more of their annual revenue from selling California residents' personal information.
c. What is the definition of personal information
    i. Information that identifies, relates to, or could reasonably be linked with the subject or their household.
    ii. E.g. name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints.
    iii. ***Excluded***: publicly available information from government records. E.g. professional license, public property records. Employee data, medical information, information from clinical trials (covered by other acts)
d. Data breach notification requirement
    i. CCPA leverages breach notification that exist under the state's general breach notification statutes.
    ii. Covers unredacted and unencrypted data.
    iii. The disclosure shall be made with minimal delay, consistent with the legitimate needs of law enforcement (can be delayed if required by law enforcement).
    iv. Should include information like: when the breach occurred, a general description of the breach, the information that was lost, and what is being done about it.
e. Violation penalty scheme
    i. Unintentional violation: maximum of 2500$ per violation
    ii. Intentional violation: maximum of 7500$ per violation
    iii. Private lawsuit in the event of data breach (non-encrypted and non-redacted personal information): 100-750$ or actual damages (whichever greater) per incident

Question 4

PDPA

- Who is protected?
  - All individuals with personal data collected, used and/or disclosed within Singapore.
- Who must comply?
  - The PDPA applies to any individual, company, association or body of persons, corporate or unincorporated, whether located in or outside Singapore (“organisations”).
- What is the definition of personal information?
  - Personal data is data, whether true or not, about an individual who can be identified: (i) from that data; or (ii) from that data and other information to which the organisation has or is likely to have access.
- Data breach notification requirement
  - Inform the PDPC as soon as practicable, no later than 72 hours (3 calendar days) after establishing that the data breach is:
    - likely to result in significant harm or impact to the individuals to whom the individual relates, or
    - of a significant scale (the breach affects the personal data of 500 or more individuals)
  - Inform Affected Individuals/Others (e.g., parents of young children) – as soon as practicable
- Violation penalty scheme
  - Fines - 10% of the offending organisation’s annual turnover in Singapore if its gross annual turnover in Singapore exceeds S$10 million, or S$1 million, whichever is higher.
  - Imprisonment - Imprisonment for up to three years

Slides for class use below

Part I: Warm up questions (submit your answers via LumiNUS-quiz by Wed noon)

1) Which of the following data is not always protected under PDPA?
   a. NRIC number
   b. Mobile phone number
   c. Personal email addresses
   d. Business contact information

2) PDPA protects an individual's personal information permanently.
   a. True
   b. False

3) Which of the following organizations does not need to comply with GDPR?
   a. Wall street journal which provides news subscription to people all over the world
   b. Google
   c. Shopee.sg
   d. None of the above

4) CCPA applies to all private organizations in California state.
   a. True
   b. False

A : tick ✅
B: cross ❌
C: slow down ⏪
D: speed up ⏩

Question 1

Right to know:

Right to delete:

Right to opt out:

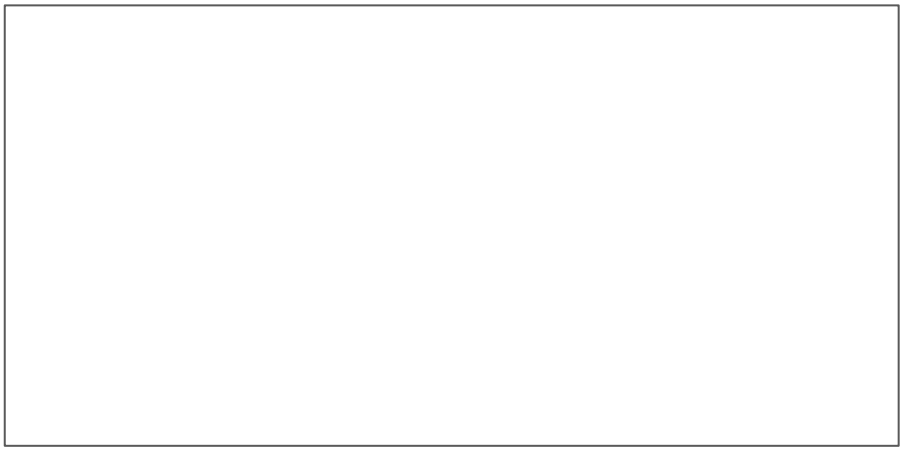
Right to non-discrimination:

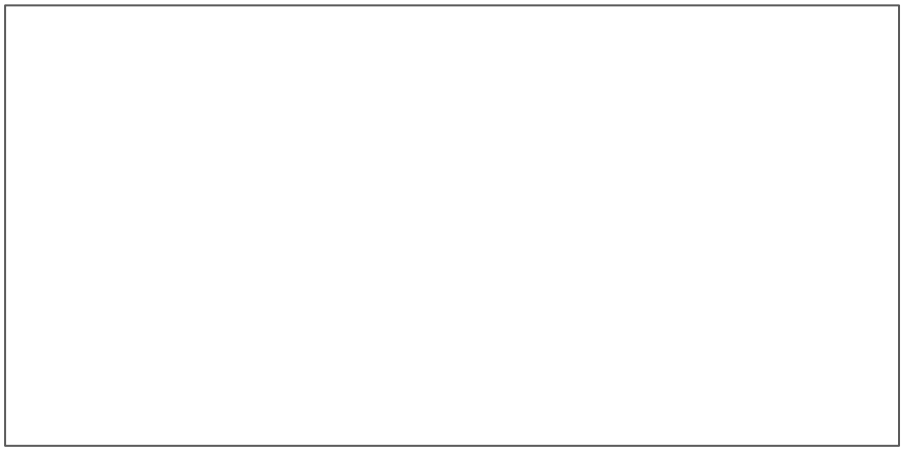
Question 2

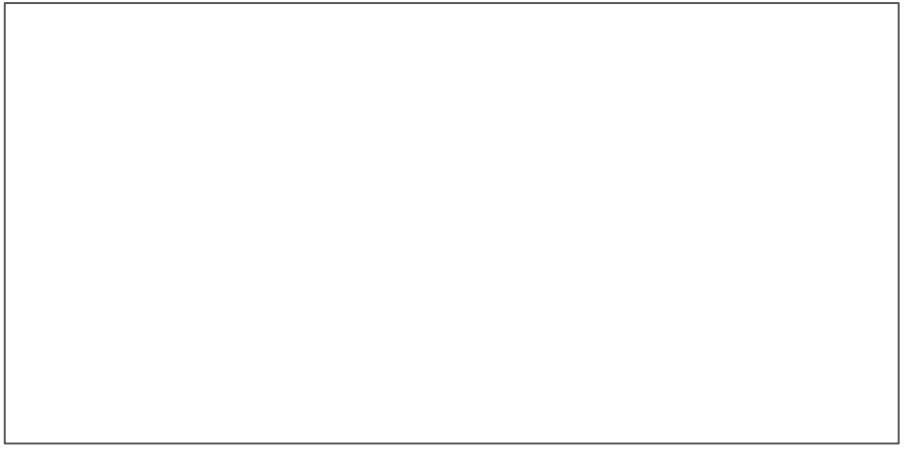
Key GDPR protection principles:

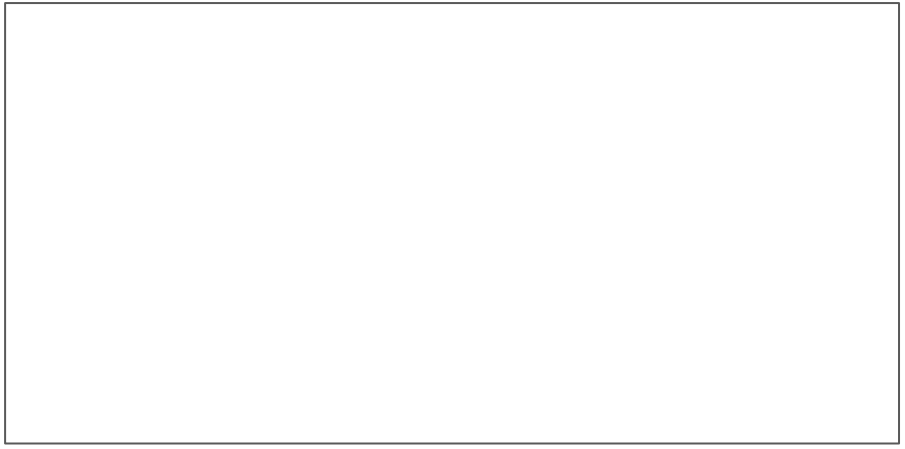
Question 3

Requirements under security of processing for GDPR:









Question 4: Who is protected?

GDPR	CCPA	PDPA

Question 4: Who must comply?

GDPR	CCPA	PDPA

Question 4: What is the definition of personal information?

GDPR	CCPA	PDPA

Question 4: Data breach notification requirement?

GDPR	CCPA	PDPA

Question 4: Violation Penalty Scheme

GDPR	CCPA	PDPA