

Tutorial 4

Global Data Protection Compliance

Presenters:

Gerard Tan

Mahmoud F M Younis

Teo Chuan Kai

PDPA

Personal Data Protection Act,
implemented on 2nd January 2013
is a **regulation** in Singapore law
that governs the collection, use,
disclosure and care of personal
data in Singapore.

PDPA (Who is protected?)

Covers personal data stored in electronic & non-electronic formats, as long as it relates to a Singaporean Entity.

Does not apply to:

1. Personal data about an individual that is contained in a record that has been in existence for at least 100 years.
2. Personal data about a deceased individual who has been dead for more than 10 years.
3. Business contact information such as an individual's name, position or title, business telephone number, business address, business email, business fax number and similar information.

PDPA (Who must comply?)

All organizations except:

1. Any public agency in relation to the collection, use or disclosure of personal data

All individuals except:

1. Any individual acting on a personal or domestic basis.
2. Any individual acting in his/her capacity as an employee with an organisation.

PDPA (Personal Data Definition)

Data about an individual who can be identified

1. from that data OR
2. from that data and other information to which the organization has or is likely to have access.

PDPA (Data breach notification requirement)

Upon determining that a data breach is notifiable, the organization must notify:

1. The Commission as soon as practicable, but in any case, no later than 3 calendar days; AND
2. where required, affected individuals as soon as practicable, at the same time or after notifying the Commission.

PDPA (Violation Penalty Scheme)

Financial Penalties

- 1) Any violations except for Do Not Call (DNC) Registry infringement = no more than 1 million
- 2) DNC Infringement:
 - a) Individual < 200k
 - b) Organization < 1million

Other Penalties

Commission may order the organization to:

- 1) Stop collecting, using or disclosing personal data in contravention of this Act
- 2) Destroy personal data collected in contravention of this Act
- 3) Provide access to or correct the personal data

What is Data Subject?

Any individuals who can be identified directly/indirectly via an identifier such as:

- Name
- ID Number
- Location Data
- Online Identifier
- A combination of ≥ 1 of the following attributes specific to the person
 - Physical
 - Physiological
 - Genetic
 - Mental
 - Economic
 - Cultural
 - Social Identity

Right to know

Data Subjects have the rights to request the following information from businesses:

- Categories of data subject's personal information collected, used, shared or sold.
 - Reasons for doing so.
- Particular pieces of data subject's personal information collected.
- Categories of sources where data subject's personal information is collected from.
- Categories of third parties whom the data subject's personal information was shared/sold.

The requested information provided by businesses, must be at least within the 12 month period prior the request.

Business must provide the information FOC.

Right to delete

Data Subjects have the rights to request for deletion of their own personal information, from businesses.

- This includes getting the business to ensure that its service providers do the same thing as well.

However, there are a few exceptions that allow businesses to reject the deletion request.

- Requester failed the verification process.
- Warranty & product recall purposes.
- Credit reporting agencies like TransUnion and Experian can still collect & disclose credit information, subject to regulation under Fair Credit Reporting Act.
- Medical information & Consumer credit reporting information are exempted from CCPA.

Requester has the right to follow up with the business to ask for the rejection reason

Right to opt-out

Data Subjects have the rights to request for the ceasing of selling their own personal information, from businesses by opting out.

- After which, businesses are not allowed to sell personal information of opted-out Data Subjects.

A minimum waiting period of at least 12 months is required for the Business before being able to ask opted-out Data Subjects to opt back into the sale of personal information.

Right to non-discrimination

Businesses **cannot treat you differently based on whether you exercised your rights under CCPA**

- Charge you different price
- Provide different level

However, if you refuse to provide/ask to delete or stop selling your personal information + that information is **critical for businesses to provide you with goods or services, business may not be obliged to complete that transaction** .

Businesses are allowed to offer promotions, discounts, deals in exchange for keeping, collecting or selling your personal information. Only if financial incentive offered is related to value of information.

CCPA (California Consumer Privacy Act 2018)

- Designed to protect the data privacy rights of citizens living in California
- Personal information definition: identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household
- Gives consumers more transparency and control over their private data and ownership, control and security of their personal information
- It forces companies to provide additional information to consumers around how their data is being collected, stored, and used

CCPA Highlights

- New privacy law broadly applicable to businesses (regardless of location) that collect personal information about California residents
- Effective January 1, 2020 (though ahead of this date further amendments are expected and the CA Attorney General is to issue implementing regulations)
- First big state-wide privacy legislation in the US.
- Substantial new rights for CA residents
- Significant operational impacts for covered business, likely require
- Significant time and effort to prepare
- Broad definitions and scope

Who does it apply to?

For profit business entities in CA that:

- Gross revenue of 25 million dollar or more
- Receives or share more then 50,000 consumers, households, or devices
- More than 50% of revenue from the sale of protected health information (PHI)
- Applies to consumer, employee, and B2B data currently
- Includes household level data and device data

CCPA Scope

- Non-profit entities are not covered
- Limited exemptions for certain regulated entities
- Partial exemption for entities and information covered by certain federal and California health info and financial privacy laws
- Not exempt from data breach private right of action
- CCPA currently exempts from its provisions certain information collected by a business about a natural person in the course of the person acting as a job applicant, **employee, owner, director, officer, medical staff member** , or contractor of a business

CCPA and Business organization

- Business required to post details on website or other public means how they're using or not using consumer data for rolling 12 months and opt out instructions
- Businesses will have to develop processes and procedures to accommodate all consumer rights including data mapping / access reports
- Requirements for businesses to reasonably safeguard consumer data
- Significant damage implications for business if fail to comply

CCPA Personal information

Explicitly includes:

- Name, contact info, government IDs, biometrics, location data, account numbers
- Employment and education history
- Purchase history, behavior, and tendencies
- Online and device IDs
- Search and browsing history and other online activities
- Activities from connected devices

Key considerations and challenges

- Expanded personal info definition (linkable to an individual or household)
- Data quality – establishing identity and resolving ambiguities
- Establishing “household” relationships
- Data sources and original acquisition channel
- Third party sharing
- California residency determination

GDPR

General Data Protection
Regulation, implemented in May
2018 is a **regulation** in EU law on
data protection and privacy in the
EU and EEA

Why?

- Enhance individuals' control and rights over their personal data
- Simplify regulatory environment regarding data for businesses & organisations

Who?

“So long as they target or collect data related to the people in the EU”

GDPR Article 3

- Data Controller (organisations that collect data from EU residents)
- Data Processor (organisation that processes data on behalf of data controller)
- Data Subject



Any 1
based
in EU

*Exception: processing of data for purely personal or household activity and affairs related to crime and taxation (GDPR, Recital 18)

What? (Personal Data)

Any information that relates to an individual who can be directly (name, email address) or indirectly identified (location information, biometric data, cookies, political opinion)

Pseudonymous data can also be considered if you can easily identify someone with it.

(Article 4)

What? (Principles)

Data protection principles (Article 5)

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- **Integrity and confidentiality**
- **Accountability**

What? (Rights of Data Subjects)

Right to be informed

Right to restrict processing

Right of access

Right to data portability

Right to rectification

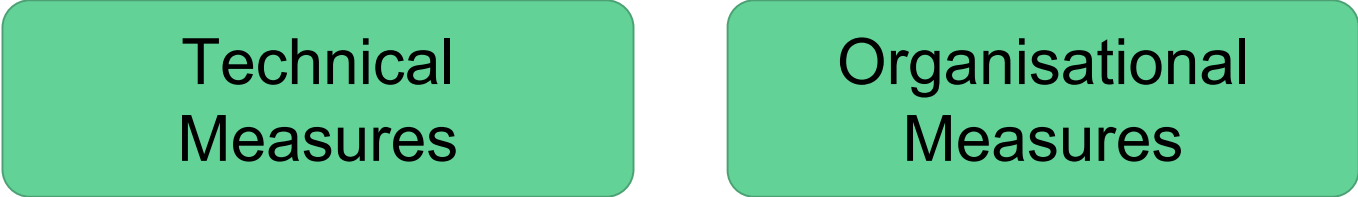
Right to object

Right to erasure

Right in relation to automated
decision making and profiling

What? (Principles)

To achieve **integrity and confidentiality** through data security, by implementing appropriate technical and organisational measures



Technical
Measures

Organisational
Measures

What? (Principles)

Accountability

GDPR states that responsibility to demonstrate compliance is on the data controllers

- Designate data protection responsibilities
- Maintain detailed documentation on collected data (how it is used, where it is stored)
- Train staff & implement organisational security measures

Data Protection by Design & Default

Everything done by organisations shall consider the data protection principles in the design of products or services (Article 25)

How? (Consent)

GDPR specifies strict rules about what constitutes consent

- Consent must be freely given, specific, informed and unambiguous
- Requests for consent must be clearly distinguishable from other matters and presented in clear and plain language
- Data subjects can withdraw previous consent
- Children <13yo can only consent with permission from parents
- Evidence of consent must be documented

How? (Data Protection Officers)

Required if:

- Public authority other than a court acting in judicial capacity
- Core activities require organisation to monitor people systematically and regularly on a large scale (eg Google)
- Core activities are large-scale processing of data relating to criminal convictions and offences

How? (Penalties)

Tier 1: Less severe infringements (Article 83)

Penalty: Fine of up to € 10 million or 2% of firm's worldwide annual revenue from preceding financial year, whichever higher

Includes:

- Controllers & processors violating rules
- Certification bodies violating evaluation and assessment processes
- Monitoring bodies mishandling infringements or complaints

How? (Penalties)

Tier 2: Violation of core principles and rights of GDPR (Article 83)

Penalty: Fine of up to €20 million or 4% of firm's worldwide annual revenue from preceding financial year, whichever higher

Includes:

- Violation of principles of data processing
- Violation of conditions for consent
- Violation of data subjects' rights
- Transfer of data to international organisation or recipient outside of EU/EEA
- Violation of member state laws
- Non-compliance with an order by supervisory authority

Cookie Settings



When you visit any of our websites, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and manage your preferences. Please note, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

Strictly Necessary



These cookies are necessary for our website to function properly and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms or where they're essential to provide you with a service you have requested. You cannot opt-out of these cookies. You can set your browser to block or alert you about these cookies, but if you do, some parts of the site will not then work. These cookies do not store any personally identifiable information.

Performance Cookies



These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site, which helps us optimize your experience. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not be able to use your data in this way.

[Cookie details](#)

Functional Cookies



These cookies enable the website to provide enhanced functionality and personalization. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies then some or all of these services may not function properly.

[Cookie details](#)

Targeting Cookies



These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

[Cookie details](#)

[Confirm my choices](#) [Accept all cookies](#) [Cancel](#)

Discussion: Cookie Prompts

What principles/rights of the GDPR are demonstrated in this situation?

Do examples like this conform to the GDPR rules on consent?

Kahoot:

CCPA vs GDPR vs PDPA

Questions?

Thank You!
