Discussion qns: (Feel free to add more info)

1) Introduce the following data subjects' rights:

a. Right to know

- The GDPR states that information must be provided to data subjects by controllers at the time when personal data are obtained, when the personal data is collected directly from data subjects
- Data controllers cannot collect and process personal data for purposes other than the ones about which the consumers were informed, unless they provide them with further information.

b. Right to delete

- Data subjects may ask to exercise their right to erasure. Erasure means that the data controller has to delete the personal data about the data subject. This right is not absolute, though, and there are times when the data controller does not have to comply.

c. Right to opt-out (https://www.dummies.com/computers/pcs/computer-security/data-protection-when-to-use-opt-in-wording/)

- Message to data subjects explaining that they must take action — such as ticking a box — to object to their data from being used in a certain way, such as objecting to their email address being used to send marketing emails.

d. Right to non-discrimination (not sure about this, below is what I found on google that might be helpful)

- *Art. 22(1) GDPR states that "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."*

2) What are the key data protection principles in GDPR?

The UK GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

3) What are the requirements under security of processing in GDPR?

1. The pseudonymisation and encryption of personal data.
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4) Regarding GDPR, CCPA, and PDPA:

a. For each regulation, who is protected?
b. For each regulation, who must comply?
c. For each regulation, what is the definition of personal information?
d. For each regulation, data breach notification requirement
e. For each regulation, violation penalty scheme

Qns (refer above)	GDPR	CCPA	PDPA
Who is protected	EU citizens and residents	People that their data is collected by the company that requires to comply CCPA	● All personal data belonging to an individual (living or deceased) is protected under the PDPA. ● Only individuals who are deceased for 10 years or more are exempt from the PDPA. ● PDPA protects three groups of individuals: (i) customers; (ii) employees; and (iii) others (eg company directors).
Who must comply	EU citizens and residents	Applies to any for-profit entity doing business in California that collects, shares, or sells California consumers' personal data, and: ● Has annual gross revenues in excess of $25 million; or ● Possesses the personal information of 50,000 or more consumers, households, or devices; or ● Earns more than half of its annual revenue from selling consumers' personal information.	Singapore organisation All private sector organisations that are engaged in data collection, processing or disclosure within Singapore, even if the organization is physically located overseas.
What is the	Data which are	Information that identifies, relates to,	data about an individual

definition of personal information?	or can be assigned to a person in any kind of way[1]	describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household	who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.
Data breach notification requirement	Notify supervisory authority no later than 72h after discovery unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subject should be informed immediately.	breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations	26B (1) A data breach is a notifiable data breach if the data 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. (2) Without limiting subsection (1)(a), a data breach is deemed to result in significant harm to an individual — (a) if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual; or (b) in other prescribed circumstances. (3) Without limiting subsection (1)(b), a data breach is deemed to be of a significant scale — (a) if the data breach affects not fewer than the prescribed number of affected individuals; or (b) in other prescribed circumstances. (4) Despite subsections (1), (2) and (3), a data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach. 26D.—(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as

			soon as is practicable, but in any case no later than 3 calendar days after the day the organisation makes that assessment. (2) Subject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also notify each affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) in any manner that is reasonable in the circumstances. (3) The notification under subsection (1) or (2) must contain, to the best of the knowledge and belief of the organisation at the time it notifies the Commission or affected individual (as the case may be), all the information that is prescribed for this purpose. (4) The notification under subsection (1) must be made in the form and submitted in the manner required by the Commission. (5) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation — (a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or (b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable

			data breach will result in significant harm to the affected individual. (6) An organisation must not notify any affected individual in accordance with subsection (2) if — (a) a prescribed law enforcement agency so instructs; or (b) the Commission so directs. (7) The Commission may, on the written application of an organisation, waive the requirement to notify an affected individual under subsection (2) subject to any conditions that the Commission thinks fit. (8) An organisation is not, by reason only of notifying the Commission under subsection (1) or an affected individual under subsection (2), to be regarded as being in breach of — (a) any duty or obligation under any written law or rule of law, or any contract, as to secrecy or other restriction on the disclosure of information; or (b) any rule of professional conduct applicable to the organisation. (9) Subsections (1) and (2) apply concurrently with any obligation of the organisation under any other written law to notify any other person (including any public agency) of the occurrence of a data breach, or to provide any information relating to a data breach.
Violation penalty scheme	Fine of up to €10 million, or 2% of the firm's worldwide annual revenue	Maximum civil penalty is $2500 for every unintentional violation and $7,500 for every intentional violation of the law.	Such organisations could face a financial penalty of up to S$1 million. So far, one of the largest

	from the preceding financial year. (more details:https://gdpr.eu/fines/)		financial penalties meted out by PDPC has been $60,000 on IT vendor Learnaholic.

1. (Eg of data in GDPR: the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address.)