1 In the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, what exception is allowed to the Access and Correction principle?

* A. Paper-based records.
* B. Publicly-available information.
* C. Foreign intelligence.
* D. Unreasonable expense.

D. Unreasonable expense. The APEC Privacy Framework's Access and Correction principle allows for exceptions when providing access to personal information or making corrections would impose an unreasonable burden or expense on the organization. In such cases, organizations may deny or limit access or correction, provided they can justify the decision as necessary and reasonable.

Such access and opportunity for correction should be provided except where: (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question; Commentary - in some situations, it may be necessary for organizations to deny claims for access and correction, and this Principle sets out the conditions that must be met in order for such denials to be considered acceptable, which include: situations where claims would constitute an unreasonable expense or burden on the personal information controller, SUCH AS WHEN claims for access are repetitious or vexatious by nature; cases where providing the information would constitute a violation of laws or would compromise security...

2 How can the privacy principles issued in 1980 by the Organisation for Economic Cooperation and Development (OECD) be defined?

* A. Guidelines governing the protection of privacy and trans-border data flows issued in collaboration with the Federal Trade Commission.
* B. Guidelines governing the protection of privacy and trans-border data flows of personal data in states that are members.
* C. Mandatory rules governing the protection of privacy and trans-border data flows within the European Union.
* D. Mandatory rules governing the protection of privacy and trans-border data flows among binding member states.

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are a set of non-binding principles intended to guide member countries in developing national policies on privacy and data protection. They aim to harmonize privacy laws while ensuring the free flow of personal data across borders.

3 Which concept is NOT an element of Cross Border Privacy Rules (CBPR)?

* A. Enforcement by Accountability Agents.
* B. Self-assessment against CBPR questionnaire.
* C. Consultation with Privacy Enforcement (PE) Authority.
* D. Dispute resolution via the Accountability Agent's compliance program.

The elements of the CBPR system include:

Enforcement by Accountability Agents: Organizations must be certified by Accountability Agents, who monitor compliance.

Self-assessment against CBPR questionnaire: Organizations conduct a self-assessment to ensure they meet CBPR requirements.

Dispute resolution via the Accountability Agent's compliance program: Accountability Agents provide mechanisms for resolving disputes.

Consultation with Privacy Enforcement (PE) Authority is not a specific element of the CBPR system. The system primarily relies on certification and enforcement by Accountability Agents and the internal compliance mechanisms of organizations.

Answer - C Elements of the CBPR System The CBPR System consists of four elements: (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement. Self-Assessment Questionnaire for Organizations The CBPR System relies on an organization’s self-assessment of their data privacy policies and practices against the requirements of 2015 APEC Privacy Framework using an APEC- recognized CBPR questionnaire (see para 21). This questionnaire will be provided by the appropriate APEC-recognized Accountability Agent, in accordance with established selection requirements

4 What term is defined by the European Commission to mean any data that relates to an identified or identifiable individual?

* A. Personally identifiable information.
* B. Sensitive information.
* C. Personal data.
* D. Identified data.

• Personal Data (EU) • EU – Any information that could be used on its own or in conjunction with other data to ID an individual. • GDPR: Personal Data • “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

5 What personal information is considered sensitive in almost all countries with privacy laws?

* A. Marital status.
* B. Health information.
* C. Employment history.
* D. Criminal convictions.

Health information is universally regarded as sensitive personal data because it can reveal highly private aspects of an individual's life and is often subject to stricter protection measures compared to other types of personal information.

6 Which jurisdiction was the first to consider IP addresses to be personal information?

* A. India.
* B. Hong Kong.
* C. The United States.
* D. The European Union.

The European Union, through its various data protection directives and regulations, notably the General Data Protection Regulation (GDPR), has recognized IP addresses as personal information because they can be used to identify individuals indirectly. This recognition has been supported by rulings from the Court of Justice of the European Union (CJEU).

The European Union (EU) was one of the first jurisdictions to consider IP addresses as personal information. The EU's data protection framework, the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, treats IP addresses as personal data in certain circumstances.

7 In the area of human rights, what separates Singapore from many other Asian countries?

* A. It is not a member of the Association of Southeast Asian Nations (ASEAN).
* B. It has not signed the International Covenant on Civil and Political Rights.
* C. It has not adopted the ASEAN Human Rights Declaration.
* D. It is not a member of the United Nations.

Singapore has not signed the International Covenant on Civil and Political Rights (ICCPR), which is a key international treaty that aims to protect civil and political rights. This sets it apart from many other countries that have ratified or acceded to the ICCPR.

8 Besides the Personal Data Protection Act (PDPA), which of the following is a potential source of privacy protection for Singapore citizens?

* A. Constitutional protections of personal information.
* B. International agreements protecting privacy.
* C. The tort of invasion of privacy.
* D. Breach of confidence law.

In Singapore, the law of breach of confidence can provide protection for personal information. This legal principle protects confidential information from being disclosed without authorization. While there is no specific tort of invasion of privacy recognized in Singapore, breach of confidence can serve as a mechanism for individuals to seek redress if their private information is disclosed improperly.

9 Which of the following would NOT be exempt from Singapore’s PDPA?

* A. A government automobile registration website.
* B. A private party room at a popular restaurant.
* C. A documentary filmed at a rock concert.
* D. A video from a store's dosed-circuit TV.

A. A government automobile registration website: Government agencies and public sector organizations are generally exempt from the PDPA.

B. A private party room at a popular restaurant: If the private party is organized by individuals for personal or domestic purposes, it may be exempt. However, if the restaurant collects and uses personal data for business purposes, it would not be exempt.

C. A documentary filmed at a rock concert: Filming a documentary at a public event like a rock concert could fall under artistic and literary purposes, which may have certain exemptions under the PDPA.

D. A video from a store's closed-circuit TV: This involves the collection of personal data by a private organization for security purposes. The store is required to comply with the PDPA regarding the handling of this data, including notification, consent, and protection measures. Therefore, this would not be exempt from the PDPA.

SCENARIO – Please use the following to answer the next question:  
Delilah is seeking employment in the marketing department of Good Mining Private Limited, an industry leader in drilling mines in Singapore. Delilah, while filling in the standard paper application form, is asked to provide details about emergency contacts, medical history, blood type and her insurance policy. These fields need to be filled in no matter which department Delilah applies to. The form also asks Delilah to expressly consent to the collection, use and disclosure of her personal data.  
A week after submitting the form, Delilah is invited by Evan, the Director of Marketing at Good Mining, to coffee. Just before Delilah leaves, she gives her business card containing her current business contact information to Evan. Evan then uses the business card to add Delilah's details to Good Mining's business development database, which is kept on a local server. Good Mining uses the database to inform people about networking and client events that Good Mining organizes.

10 Why is it legal for Evan to add the information on Delilah's business card to the business development database?

* A. Because Delilah "consented" to her business contact information being used by Good Mining by passing it to Evan voluntarily.
* B. Because any business contact information can be freely used, collected or disclosed by Good Mining.
* C. Because Good Mining does not export the information to a cloud vendor.
* D. Because Delilah initiated the relationship with Good Mining.

In this scenario, Delilah provided her business card to Evan voluntarily, which can be interpreted as implied consent for Evan to use her business contact information for business-related purposes. This falls in line with the principles of implied consent under Singapore's PDPA, where an individual voluntarily providing their business contact information for business purposes is deemed to have consented to its use for those purposes.

11 Why is Good Mining Private's standard form NOT compliant with Singapore's data protection law?

* A. It is not available in an electronic format.
* B. It does not contain the contact information for the HR manager.
* C. It asks for Delilah's consent to use and disclose her personal data.
* D. It asks for details that are not relevant to the job Delilah is applying for.

Under Singapore's Personal Data Protection Act (PDPA), organizations must ensure that they only collect, use, and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. Collecting details about Delilah's emergency contacts, medical history, blood type, and insurance policy for a marketing department job application is likely to be considered excessive and irrelevant to the job she is applying for. Thus, the form is not compliant with the PDPA because it asks for more information than is necessary for the job application process.

The reason why Good Mining Private's standard form is NOT compliant with Singapore's data protection law is option D, as it asks for details that are not relevant to the job Delilah is applying for. Singapore's Personal Data Protection Act (PDPA) requires that organizations only collect, use, and disclose personal data for purposes that are reasonable and relevant. Asking for information such as emergency contacts, medical history, blood type, and insurance policy is not necessary or relevant to Delilah's job application in the marketing department. Therefore, it is considered excessive collection of personal data, which is a violation of the PDPA. Additionally, the collection and use of Delilah's business card for purposes other than what was explicitly agreed to by Delilah, which was to contact her for coffee, may also be a violation of the PDPA.

D- breach of confidence law. Singapore provides very little legal protection to privacy outside the new PDPA. It has no explicit constitutional protections of privacy, and it is not a party to any enforceable international agreements protecting privacy. It is uncertain whether there is tort protection against harassment, but otherwise there is no tort of invasion of privacy. Some protection is provided by breach of confidence law.

B - International Covenant on Civil and Political Rights (ICCPR). “The Singaporean government missed yet another opportunity to address many human rights concerns raised by the international community. Singapore can no longer ignore the important civil and political rights that its citizens should enjoy.” Karim Lahidji, FIDH President The government did not accept any of the

12 Which of the following does Singapore's PDPC NOT have the power to do?

* A. Order an organization to stop collecting personal data.
* B. Order an organization to destroy collected personal data.
* C. Order an organization to award compensation to a complainant.
* D. Order an organization to pay a financial penalty to the government.

While the PDPC has the authority to order organizations to stop collecting personal data, destroy collected personal data, and pay financial penalties to the government, it does not have the power to order organizations to award compensation to complainants. Compensation claims would need to be pursued through the courts.

Enforcement of the Data Protection If the PDPC finds that an organisation has breached any of the PDPA provisions, we will direct the organisation to take steps to ensure compliance such as: Stop collecting, using or disclosing personal data in contravention of the Act; Destroy personal data collected in contravention of the Act; Provide access to or correct the personal data; and/or Pay a financial penalty.

It should however be noted that the Commission is not empowered to award damages to a complainant. As such, the Commission will generally prefer to take other measures (such as facilitation and alternative dispute resolution mechanisms like mediation) to encourage the parties to discuss the issues in a complaint and find a mutually acceptable resolution, which may include compensation.

The Commission is not empowered to award damages or other relief noted above to a complainant, persons who suffer loss or damage as a result of a contravention of the PDPA may commence civil proceedings directly. In general, such persons may wish to obtain legal advice in relation to their claim and possible civil proceedings.

<https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/enforcement-of-the-act>

SCENARIO – Please use the following to answer the next question:  
Singabank is a boutique bank in Singapore. After being notified during the hiring process, Singabank employees are subject to constant and thorough monitoring and tracking through CCTV cameras, computer monitoring software and keyboard loggers. Singabank does this to ensure its employees are complying with Singabank's data security policy. Bigbank is now considering acquiring Singabank's retail banking division. As part of its due diligence, Bigbank is seeking for Singabank to disclose to it all of its surveillance material on its employees, whether or not they are part of the retail banking division. Jimmy works in Singabank's investment banking division.

13 What would make Singabank's monitoring of its employees illegal?

* A. If the employees did not explicitly consent to it.
* B. If the bank's data security policy was being overhauled.
* C. If the bank collected employees' sensitive personal information.
* D. If the employees were not provided contact information to ask questions about the monitoring.

Under Singapore's Personal Data Protection Act (PDPA), organizations must obtain consent from individuals before collecting, using, or disclosing their personal data, unless an exception applies. This includes monitoring and tracking employees. If Singabank did not obtain explicit consent from its employees for such extensive monitoring, this would make the practice illegal. Explicit consent is particularly important in cases involving intrusive surveillance methods like CCTV cameras, computer monitoring software, and keyboard loggers.

14 Assuming the monitoring was legal, can Singabank disclose Jimmy's personal data to Bigbank?

* A. No, because Jimmy is not in the division that Bigbank seeks to acquire.
* B. No, because the data was collected for the express purpose of complying with Singabank's privacy policies.
* C. Yes, if Singabank informs Jimmy of the disclosure of his personal data before it occurs.
* D. Yes, if Jimmy's personal data is necessary for Bigbank to determine whether to proceed with the acquisition.

Singabank's disclosure of Jimmy's personal data to Bigbank would not be justified because Jimmy is not part of the retail banking division that Bigbank is considering acquiring. Sharing his personal data would likely be considered excessive and unrelated to the specific purpose of the due diligence process for the acquisition of the retail banking division. Under Singapore's PDPA, organizations must ensure that personal data is only disclosed for purposes that a reasonable person would consider appropriate in the circumstances. Disclosing data beyond what is necessary for the acquisition would not meet this standard.

D as this would likely fall under the business asset transaction exception from consent obligation under the PDPA.

15 In which of the following cases would a Singaporean be prevented from accessing information about herself from an organization?

* A. The information was collected in the previous 12 months.
* B. The information is related to an individual's credit rating.
* C. The cost of providing the information proved to be unreasonable.
* D. Any personal information about others has been deleted from the document.

Under Singapore's Personal Data Protection Act (PDPA), an organization may refuse access to personal data if the burden or expense of providing access would be unreasonable to the organization. This is one of the exceptions to the right of access, ensuring that the process does not place an undue financial or operational burden on organizations.

The exceptions specified in the Fifth Schedule include the following matters: Organisations should note that they are not required to provide access if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual’s interest or if the request is otherwise frivolous or vexatious. j) any request — i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests; ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual’s interests;

16 Which of the following principles of the OECD guidelines and Council of European Convention principles does Singapore's PDPA incorporate?

* A. Disclosures to third parties included in access requests.
* B. Additional protections for sensitive personal data.
* C. The ability to opt-out from direct marketing.
* D. The right of deletion of data on request.

Under Singapore's PDPA, individuals have the right to opt-out of receiving direct marketing communications. This aligns with the principles of the OECD guidelines and the Council of Europe Convention, which emphasize individuals' control over their personal data, including the ability to opt-out of unwanted direct marketing activities.

A is wrong as this principle is not explicitly mentioned in the OECD guidelines or the Council of European Convention principles. B is wrong as there is no concept of sensitive personal data under the PDPA. D is also wrong as there is no right of deletion under the PDPA. C is correct as under the PDPA, the data subjects have the right to withdrawal of consent from direct marketing. Both the OECD guidelines and the Council of European Convention principles emphasize the importance of individuals having the ability to opt-out from direct marketing.

SCENARIO – Please use the following to answer the next question:  
B-Star Limited is a Singapore based construction company with many foreign construction workers. B-Star's HR team maintains two databases. One (the "simple database") contains basic details from a standard in-processing form such as name, local address and mobile number. The other database (the "sensitive database") contains information collected by the HR Department as part of Annual Review Interviews. With the workers' cooperation, this database has expanded to include far-reaching sensitive information such as medical history, religious beliefs, ethnicity and educational levels of immediate family members. Carl left B-Star's employment yesterday, and has flown back home, rendering him unreachable. Today B-Star, without Carl's consent, wants to conduct research using Carl's medical records in the sensitive database.

17 Can B-Star legally conduct this research using Carl's medical data?

* A. Yes, because Carl gave his consent for his sensitive personal data to be collected during his employment.
* B. No, an organization is not allowed to use sensitive personal data without an individual's consent unless absolutely necessary.
* C. No, because the research is taking place after Carl has left B-Star's employment.
* D. Yes, if the research is deemed to be in the public interest.

Under the PDPA, the use of sensitive personal data without consent is strictly regulated and typically only permissible under specific exceptions, such as if it is necessary for a medical emergency or for legal purposes. Conducting research would generally require explicit consent from the individual, and the fact that Carl is no longer employed by B-Star does not change this requirement.

Should be D, this is an exemption provided under Schedule 2 of the PDPA

18 A Singapore employer can do all of the following without obtaining an employee's consent EXCEPT?

* A. Share an employee's personal data with a company that provides financial planning.
* B. Disclose personal health data to a public agency during a health crisis.
* C. Use computer monitoring software on an employee's computers.
* D. Use closed-circuit television surveillance in the workplace.

Under Singapore's Personal Data Protection Act (PDPA), sharing an employee's personal data with a third party, such as a financial planning company, requires the employee's consent. The other actions listed can typically be done without consent under specific conditions, such as for security purposes (CCTV surveillance), monitoring employee productivity (computer monitoring software), or in cases of public interest (disclosure of health data during a health crisis).

19 Which control is NOT included in the requirements established by the Monetary Authority of Singapore (MAS) for financial institutions in order to deter money-laundering and financial aid to terrorism (AML/CFT)?

* A. Identifying and knowing customers.
* B. Sharing personal information with the PDPC.
* C. Conducting regular reviews of customer accounts.
* D. Monitoring and reporting suspicious financial transactions.

The MAS requirements for financial institutions to deter money laundering and combat the financing of terrorism typically include controls such as identifying and knowing customers (A), conducting regular reviews of customer accounts (C), and monitoring and reporting suspicious financial transactions (D). However, sharing personal information with the Personal Data Protection Commission (PDPC) is not a standard requirement under AML/CFT regulations.

The AML/CFT requirements for banks: Risk assessment and risk mitigation. Customer due diligence. Reliance on third parties. Correspondent banking and wire transfers. Record keeping. Suspicious transaction reporting. Internal policies, compliance, audit and training. At the regulatory level, the PDPC, MAS and CSA can work closely and collaborate with each other to enhance the data protection 1.6 In this respect, we recommend: (a) Collaborative reporting between FIs and MAS, CSA and PDPC (collectively, the “regulatory agencies”), where notifying MAS and/or PDPC in the event of a data breach will suffice. (b) Collaborative investigating between FIs and the regulatory agencies, where only MAS and/or PDPC will investigate should the need arise. (c) Greater coordination between the regulatory agencies.

MAS does not require sharing of personal information with the PDPC. Identifying and knowing customers, on the other hand, is part of KYC requirements that is integral to PMLTF.

20 All of the following are guidelines the PDPC gives about anonymised data EXCEPT?

* A. Anonymised data is not personal data.
* B. Any data that has been anonymised bears the same risks for re-identification.
* C. Data that has been anonymised satisfies the "cease to retain" requirement of Section 25.
* D. Organizations should consider the risk of re-identification if it intends to publish or disclose anonymised data.

This statement is incorrect as it suggests that all anonymised data inherently carries the same risk of re-identification, which is not the case. The PDPC acknowledges that the risk of re-identification can vary depending on how effectively the data has been anonymised and other contextual factors. The other options correctly reflect the PDPC's guidelines on anonymised data.

Anonymising data doesn't necessarily satisfy the requirement to cease retention. Ceasing retention typically refers to deleting or securely disposing of personal data once it's no longer needed for its original purpose.

21 Under what circumstances are smart identity cards required of Hong Kong citizens?

* A. When opening bank accounts.
* B. When using public transit systems.
* C. When seeking government services.
* D. When making substantial purchases.

Smart identity cards in Hong Kong are used for accessing various government services, among other functions. They serve as a proof of identity and are necessary for interactions with government departments.

22 Hong Kong's Personal Data (Privacy) Ordinance (PDPO) was primarily inspired by which of the following?

* A. Asia's APEC Privacy Framework.
* B. Macau's Personal Data Protection Act.
* C. South Korea's Public Agency Data Protection Act.
* D. Europe's Data Protection Directive (Directive 95/46/EC).

The PDPO was modeled after the principles and frameworks established in the European Data Protection Directive, reflecting similar standards and protections for personal data.

Origins of, and influences on, the Ordinance The Ordinance’s enactment was not prompted by any significant public demands or major controversy, but was led by the then colonial administration, influenced by local elite opinion. It was a positive and not a reactive process, influenced by European developments and their potential effect on trade with Hong Kong. The history of the Ordinance’s development shows that the Hong Kong government was concerned about possible limits on personal data flows from Europe as early as the 1981 Council of Europe Data Protection Convention BUT heightening in the early 1990s as the European Union (EU) Data Protection Directive developed. From 1989 the HKLRC was given a very broad reference on privacy protection, and following public consultations published recommendations for data protection legislation, the majority of which were embodied in the 1995 Ordinance.

23 Hong Kong's definition of a data user in the original PDPO applies to all of the following EXCEPT?

* A. Trust corporations.
* B. Third-party processors.
* C. Private sector organizations.
* D. Limited liability partnerships.

The PDPO defines a data user as a person or organization that controls the collection, holding, processing, or use of personal data. This typically includes trust corporations, private sector organizations, and limited liability partnerships. However, third-party processors that process data on behalf of a data user are not considered data users themselves under the original PDPO.

Data User is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data. Data user (Controller ) Data Intermediary ( Vendor , Data processor ) The Data Intermediary is referred to differently depending upon the country or jurisdiction. In Singapore, it is data intermediary. In EU – the data processor, And in the United States / India – a data processor is typically referred to as a vendor, service provider or a third-party service provider

A party who is only processing the data as agent for another person (a processor) is not a data user.

24 In what way are Hong Kong citizens protected from direct marketing in ways that India and Singapore citizens are not?

* A. Subscribers must have explicitly indicated that they did not object to their data being collected and used for marketing purposes.
* B. Subscribers can opt out of the use of their data for marketing purposes after collection by withdrawing consent.
* C. Data subjects must be notified on a website if their data is being used for marketing purposes.
* D. Data subjects are protected from the secondary use of personal data for marketing purposes.

Under Hong Kong's Personal Data (Privacy) Ordinance (PDPO), organizations are required to obtain explicit consent from individuals before using their personal data for direct marketing purposes. This means that subscribers must have explicitly indicated that they do not object to their data being used for marketing. This level of explicit consent is a higher standard compared to some of the protections in India and Singapore.

SCENARIO – Please use the following to answer the next question:  
Zoe is the new Compliance Manager for the Star Hotel Group, which has five hotels across Hong Kong and China. On her first day, she does an inspection of the largest property, StarOne. She starts with the hotel reception desk. Zoe sees the front desk assistant logging in to a database as he is checking in a guest. The hotel manager, Bernard, tells her that all guest data, including passport numbers, credit card numbers, home address, mobile number and other information associated with a guest's stay is held in a database. Bernard tells her not to worry about the security of the database because it is operated for Star Hotels by a local service provider called HackProof, who therefore are responsible for all the guest data.  
Zoe notices what looks like a CCTV camera in the corner of the reception area. Bernard says they record all activity in the lobby. In fact, last Tuesday he had received a data access request from a lawyer requesting a copy of footage of all lobby activity for the preceding month. The lawyer's covering letter said that his client has never visited the hotel herself, but is investigating whether her husband has been doing so without her knowledge.  
Zoe and Bernard head up to the hotel spa. The spa is independently owned by a company called Relax Ltd. Bernard explains that Relax Ltd is a small company and, as they don't have their own database, they transfer data about the spa guests to StarOne staff so that they can upload the data into the HackProof system. Relax Ltd staff can then login and review their guest data as needed.  
Zoe asks more about the HackProof system. Bernard tells her that the server for the Hong Kong hotels is in Hong Kong, but there is a server in Shenzhen that has a copy of all the Hong Kong hotel data and supports the properties in China. The data is in China for back up purposes and also is accessible by staff in the China hotels so they can better service guests who visit their hotels in both territories.

25 How should Bernard respond to the lawyer’s request for the CCTV footage?

* A. Decline to turn over the footage as it is not a valid data access request.
* B. Provide a copy of the footage within 40 days as it is a data access request.
* C. Provide a copy of the footage to the lawyer under the exemption for legal professional privilege.
* D. Decline to turn over the footage as there is no basis for it to be disclosed under the exemption for prevention or detection of crime.

The lawyer's request does not constitute a valid data access request under Hong Kong's Personal Data (Privacy) Ordinance (PDPO) because the lawyer's client is not the data subject in the footage. Data access requests typically need to be made by the individual whose personal data is being requested, or by someone authorized to act on their behalf. In this case, the request is for footage to investigate the client's husband, who is the actual data subject in the footage.

Exemptions While data privacy is an important right, the interests protected under PDPO have to be balanced against other important rights or public interest. PDPO provides a number of exemptions from some compliance requirements under particular circumstances. Examples include crime prevention or prosecution, security and defence, statistics and research, news activity, protecting a data subject’s health etc. There is also an exemption if the use of personal data is required or authorised by law or court order or is required for exercising or defending legal rights in Hong Kong. Prevention or detection of crime According to section 58 of the Ordinance, personal data held for the purpose of prevention or detection of a crime may be exempt from the provisions in respect of data-access requests (DPP 6 and section 18(1)(b) of the Ordinance) and restrictions on the use of personal data (DPP 3).

26 HackProof reports to Zoe that a copy of the entire guest database has been exfiltrated by a hacker. What is Zoe's best course of action?

* A. Zoe must immediately notify all guests, the police and the Privacy Commissioner of the breach.
* B. Zoe does not need to do anything as there is no mandatory breach notification requirement in Hong Kong.
* C. Zoe must report the breach to the Privacy Commissioner and make an action plan together with the Commissioner.
* D. Zoe should consider if there is a real risk of harm to the guests and take appropriate action based on her assessment.

While Hong Kong does not have a mandatory data breach notification requirement, it is best practice to assess the risk of harm to the affected individuals. If there is a real risk of significant harm, Zoe should notify the affected guests and take appropriate steps to mitigate any potential damage. She should also consider informing the Privacy Commissioner, although it is not mandatory, to demonstrate transparency and responsibility in handling the breach.

HANDLING DATA BREACHES The following steps are recommended when handling a data breach. Step 1: Immediate gathering of essential information Step 2: Containing the data breach Step 3: Assessing the risk of harm Step 4: Considering giving data breach notifications Step 5: Documenting the breach Assessing the risk of harm Once all essential information has been gathered, the data users should then ensure that they understand the risks of harm that may be caused to the affected individuals, so that they can take steps to limit the impact.

Notifying the data subjects is next if the breach has serious problems like ...The possible harm caused by a data breach may include: • Threats to personal safety • Identity theft • Financial loss • Humiliation or loss of dignity, damage to reputation or relationships • Loss of business or employment opportunities.

27 Assuming that Section 33 is in force, which of the following would NOT help Zoe to facilitate the cross-border transfer from Hong Kong to China?

* A. Consent of the guest in writing to the transfer.
* B. Amending StarOne's privacy policy to refer to the transfer.
* C. Putting in place Model Clauses between the relevant entities.
* D. China being included as a "White List" country for data transfer.

Amending the privacy policy to refer to the transfer does not provide sufficient legal safeguards or meet the specific requirements under Section 33 for cross-border data transfers. The other options—obtaining the guest's written consent, putting in place Model Clauses, and ensuring China is included as a "White List" country—are recognized methods to facilitate cross-border data transfers and ensure compliance with the PDPO.

A is permitted under section 33(2)(c), D is permitted under section 33(2)(a), and putting in the model clauses is permitted under section 33(2)(f).

28 Members of Relax Ltd's staff are concerned about the data sharing with StarOne.  
How should Zoe respond to their concerns?

* A. Inform the staff that Relax Ltd can transfer the data to StarOne given they are in the same premises and guests would reasonably expect that.
* B. Inform the staff that Relax Ltd should not transfer the data to StarOne without a privacy notice identifying StarOne as a class of transferee.
* C. Inform the staff that Relax Ltd should not transfer the data to StarOne without the guest's opt-in consent to do so.
* D. Inform the staff that Relax Ltd can transfer the data as Section 33 is not in force.

This ensures that the data transfer complies with data protection laws and respects the privacy of the guests, as the guests must be informed and give explicit consent for their personal data to be shared with another entity.

Under Hong Kong's Personal Data (Privacy) Ordinance (PDPO), it is important to inform data subjects about the transfer of their personal data and the parties to whom their data may be transferred. Relax Ltd should provide a privacy notice that identifies StarOne as a class of transferee, ensuring transparency and compliance with the PDPO requirements. This approach ensures that guests are adequately informed about who will have access to their personal data and for what purposes, thereby addressing the concerns of Relax Ltd's staff.

29 Increases in which of the following were a major reason for the enactment of Hong Kong's Amendment Ordinance in 2012?

* A. Direct marketing practices.
* B. Law enforcement requests.
* C. Biometric authentication.
* D. Data breach reports.

The 2012 amendments to Hong Kong's Personal Data (Privacy) Ordinance (PDPO) were largely driven by concerns over direct marketing practices. These amendments introduced stricter requirements for obtaining consent for direct marketing and increased penalties for non-compliance, aiming to better protect individuals' privacy in the context of direct marketing activities.

30 The "due diligence" exemption in Hong Kong's PDPO was meant to apply to?

* A. Third-party data processors located in foreign countries.
* B. Companies researching the viability of business mergers.
* C. Service providers hosting customer information in the cloud
* D. Direct marketers acting in the best interest of their company.

This exemption allows organizations to process personal data without consent during due diligence activities for business transactions such as mergers, acquisitions, or other corporate restructuring, where it is necessary to assess the viability of the transaction.

4.15 The question may arise as to whether the requirements under this Part applies to the situation where personal data is provided to another person due to a merger or business amalgamation involving a sale of business or shares. The short answer is that the requirements under this Part do not apply if the personal data provided is not for use in direct marketing. Otherwise, consent has to be obtained from the data subject. Data users should be mindful that if the provision is for use in direct marketing under the guise of a merger or acquisition, they are still liable under the Ordinance.

31 Hong Kong's New Guidance on Direct Marketing clarified that direct marketing rules under the new regime do NOT apply if what condition exists?

* A. The data subject’s personal data is collected from public registers or third parties.
* B. The products or services are being offered by the organization's parent company.
* C. The data subject has already given consent for other services offered by the company.
* D. The products or services are being offered for the exclusive use of an individual's organization.

The direct marketing rules generally apply to the use of personal data collected directly from data subjects. However, if the personal data is collected from public registers or third parties, the stringent requirements of the new direct marketing regime may not apply in the same way, as long as the use of such data complies with other relevant provisions of the Personal Data (Privacy) Ordinance (PDPO).

SCENARIO – Please use the following to answer the next question:  
Fitness For Everyone ("FFE") is a gym on Hong Kong Island that is affiliated with a network of gyms throughout Southeast Asia. When prospective members of the gym stop in, call in or submit an inquiry online, they are invited for a free trial session. At first, the gym asks prospective clients only for basic information: a full name, contact number, age and their Hong Kong ID number, so that FFE's senior trainer Kelvin can reach them to arrange their first appointment.  
One day, a potential customer named Stephen took a tour of the gym with Kelvin and then decided to join FFE for six months. Kelvin pulled out a registration form and explained FFE's policies, placing a circle next to the part that read "FEE and affiliated third parties" may market new products and services using the contact information provided on the form to Stephen "for the duration of his membership." Stephen asked if he could opt-out of the marketing communications. Kelvin shrugged and said that it was a standard part of the contract and that most gyms have it, but that even so Kelvin's manager wanted the item circled on all forms. Stephen agreed, signed the registration form at the bottom of the page, and provided his credit card details for a monthly gym fee. He also exchanged instant messenger/cell details with Kelvin so that they could communicate about personal training sessions scheduled to start the following week.  
After attending the gym consistently for six months, Stephen's employer transferred him to another part of the Island, so he did not renew his FFE membership.  
One year later, Stephen started to receive numerous text messages each day from unknown numbers, most marketing gym or weight loss products.  
Suspecting that FFE shared his information widely, he contacted his old FFE branch and asked reception if they still had his information on file. They did but offered to delete it if he wished. He was told FFE's process to purge his information from all the affiliated systems might take 8 to 12 weeks. FFE also informed him that Kelvin was no longer employed by FFE and had recently started working for a competitor. FFE believed that Kelvin may have shared the mobile contact details of his clients with the new gym and apologized for this inconvenience.

32 Assuming that Kelvin received a commission for sharing his former client list with the new employer, and the new employer used Stephen's data to engage in direct marketing to Stephen, which of the following penalties could Kelvin face under Part VI A of the Ordinance?

* A. No penalty, as FFE and the new employer are the responsible parties.
* B. Violation of the terms of his employment agreement.
* C. A maximum $500,000 HKD fine.
* D. Up to five years imprisonment.

Under Part VI A of Hong Kong's Personal Data (Privacy) Ordinance (PDPO), disclosing personal data obtained without consent and for profit or malicious intent is considered a serious offense. This could result in substantial penalties, including imprisonment of up to five years and a maximum fine of $1,000,000 HKD.

D mentioned in Part VI Up to 5 yrs imprisonment or fine of HKD1mil max for breach of direct marketing rules for gain. Not for gain - max 3 yrs imprisonment or HKD500K fine.

33 Which of the following FFE data retention policies would be permitted under Section 26 of the Personal Data (Privacy) Ordinance and Hong Kong Data Protection Principle 2 regarding accuracy and retention?

* A. Retain the data of members who have been suspended for non-payment, in the event that the data is needed to seek compensation in a court of law.
* B. Retain all member data and documents in original form for two years after account termination, to better inform marketing efforts focused on re-activating accounts of former customers.
* C. Retain an anonymous data set after account termination indicating dates of membership, age, and other statistical data, to be included in aggregate reports about gym membership trends.
* D. Retain copies of files of customers who utilized personal trainer services for six months after account termination, to allow trainers to respond to inquiries from personal physicians about training-related injuries.

This policy involves retaining data in an anonymous form, which is not considered personal data under the PDPO. As the data is anonymized, it no longer identifies individuals, and thus retaining it for aggregate reporting purposes does not conflict with the principles of data protection concerning accuracy and retention.

DPP2 Accuracy and Duration of Retention DPP2 requires data users to take all practicable steps to ensure that personal data is accurate and is not kept longer than is necessary for the fulfillment of the purpose for which the data is used. If you engage a data processor for handling personal data of other persons, you should adopt contractual or other means to ensure that the data processor comply with the mentioned retention requirement. Section 26 of PDPO requires data users to take all practicable steps to erase personal data that is no longer required for the purpose for which the data is used, unless erasure is prohibited by law or is not in the public interest. Section 26 could be engaged when a data user fails to respond to a complaint or request from a data subject for erasure of personal data. This situation attracts a heavier criminal gravity than just keeping the data longer than is necessary under DPP2. Contravention of the requirement under section 26 is an offence,punishable by a fine of up to HK$10,000

34 Which of the following practices would likely violate Hong Kong's Data Protection Principle 1 regarding data collection?

* A. FFE's collection of full name from prospective clients.
* B. FFE affiliates' receipt of Stephen's contact information.
* C. FFE's collection of age and HKID from prospective clients.
* D. FFE's collection of Stephen's messenger cell details through Kelvin.

Hong Kong's Data Protection Principle 1 states that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user, and that the data collected should be adequate but not excessive in relation to that purpose.

Collecting age and Hong Kong ID (HKID) numbers from prospective clients who are merely inquiring about a free trial session could be seen as excessive and not directly necessary for arranging a trial session or responding to an inquiry. This information might be more relevant at a later stage (such as formal membership registration), but not at the initial inquiry stage.

Answer C - - DP1 - Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred DP1 - Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred

35 Which of the following types of text messages are permissible, regardless of Stephen's withdrawal of consent?

* A. From the FFE retention department, offering a special discount for reactivating membership.
* B. From health care services provided by Hong Kong's Hospital Authority or Department of Health.
* C. From an FFE affiliate that provides a mechanism to opt out of further communications by reply-texting "OO."
* D. From an FFE affiliate in the region Stephen was transferred to, offering services similar to those he purchased previously.

Messages from health care services provided by Hong Kong's Hospital Authority or Department of Health are typically exempt from direct marketing regulations due to their public interest and health-related nature. These messages are often considered necessary for public health and safety and are therefore not subject to the same consent requirements as commercial marketing messages.

The other options involve commercial or marketing communications, which would not be permissible without Stephen's consent, especially after he has withdrawn consent.

Division 2—Use of Personal Data in Direct Marketing 35B. Application This Division does not apply in relation to the offering, or advertising of the availability, of— (a) social services run, subvented or subsidized by the Social Welfare Department; (b) health care services provided by the Hospital Authority or Department of Health; or (c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of— (i) the individual to whom the services are intended to be provided; or (ii) any other individual.

DPP3 Use of Data DPP3 prohibits the use of personal data for any new purpose which is not or is unrelated to the original purpose when collecting the data, unless with the data subject’s express and voluntary consent. A data subject can withdraw his/her consent previously given by written notice. Regarding restrictions on use of personal data, Part 6A of the PDPO further requires that data users must obtain informed consent before using a data subject’s personal data for direct marketing or transferring the data to a third party for direct marketing. The consent must be an explicit indication by the data subject and broadly covers an indication of no objection. In other words, silence cannot constitute consent.

36 In Hong Kong's revised Breach Guidance Note of 2015, what course of action did the Commissioner recommend that companies take immediately after experiencing a breach?

* A. Proceed under the assumption that the breach is a threat to personal safety.
* B. Enlist the aid of law enforcement to determine the cause of the breach.
* C. Quickly issue a notification to the data subjects affected by the breach.
* D. Immediately gather essential information in relation to the breach.

The guidance emphasizes the importance of quickly understanding the nature and scope of the breach by gathering essential information. This step is crucial for assessing the potential impact, determining the appropriate response, and deciding on further actions, such as notification to affected data subjects and relevant authorities.

Should be D: The commissioner recommends the following action plan: Step 1: Immediately gather essential info relating to breach Step 2: Contact interested parties and adopt measures to contain breach Step 3: Assess the risk of harm Step 4: Consider giving a data breach notification.

37 How was the Supreme Court's ruling in the Maneka Gandhi v Union of India case significant to Indian law?

* A. It expanded the interpretation of right to life under Article 21 of the Constitution.
* B. It established that privacy is a fundamental right granted by the Constitution under Article 21.
* C. It upheld that the impounding of passports for "public interest" is allowable under Section 10(3)(c) of the Passports Act.
* D. It ruled that under Article 32 of the Constitution individuals may file writ petitions when they feel their rights were violated.

The ruling in Maneka Gandhi v Union of India (1978) was a landmark decision that broadened the scope of Article 21 of the Indian Constitution. The Supreme Court held that the right to life and personal liberty is not confined to mere physical existence but includes the right to live with human dignity and all that goes along with it, such as the right to travel abroad. This case also established the principle that any law affecting personal liberty must pass the tests of reasonableness and fairness, thereby enhancing the protection of fundamental rights in India.

The decision held by the Supreme Court has been a guiding light in understanding the aspects of fundamental rights mentioned part-ⅲ of the Indian Constitution. This case deals with the principles of natural justice enshrined under Article 14 and 21 of the Indian Constitution. Before this case article 21 only deals with assuring the right to life and personal liberty against the arbitrary actions of the executive but after the judgment of this case the scope of article 21 has been expanded and it take actions against the legislative also for the violation of fundamental rights mentioned under article 21. The ruling of Maneka Gandhi case was handed down by the seven-judge bench of the The Maneka Gandhi case is considered as the land mark case in the history of Indian Legal system because this case has widened the scope of Article 21 of the Indian constitution which provides the provision for protection of life and personal liberty

This case became a landmark judgment for highlighting the importance of the right to life as an expansive right.

38 Which of the following entities do NOT fall under India's Right to Information Act of 2005?

* A. High courts.
* B. State legislatures.
* C. Law enforcement agencies.
* D. National Security Guard.

India's Right to Information Act of 2005 provides citizens with access to information under the control of public authorities to promote transparency and accountability. However, certain security and intelligence organizations, including the National Security Guard, are exempt from the provisions of the RTI Act under Section 24, except in cases involving allegations of corruption or human rights violations.

In the Central Act, section 8(1) lists all of the exemptions. • National Security or Sovereignty: As explained above, there is some information, which relates to India's national security, which could genuinely cause harm if it was released to the public. For example, information published during a conflict, detailing the number of soldiers defending a boundary, where they were positioned or their strategic plans. However, it would not be appropriate to use this exemption simply to keep a contract for the purchase of an air force fighter jet secret. This is common commercial information which should be made public to reduce the likelihood of corruption tainting the procurement process and should not be withheld simply because it relates to defense.

The ‘right to information’ provided by the 2005 national legislation has a broad scope, covering ‘information held by or under the control of any Public Authority’. ‘Public authority’ includes anybody established under the Constitution, or Centre or state law, or under delegated legislation, and includes bodies owned or controlled by government or directly or indirectly substantially Financed by government (even if they are NGOs). The reach of the legislation is therefore to all tiers of government and somewhat beyond that. In 2004 India’s Supreme Court conclusively interpreted article 19(1)( a) of the Constitution of India to impliedly include the right to information in the constitutional guarantees of freedom of speech and expression (People’s Union for Civil Liberties v Union of India), Five years before a similar conclusion was reached in Europe. National legislation was then enacted by the Centre as the Right to Information Act 2005 (RITA).

It is extremely positive that the Central Act makes all of the exemptions contained in section 8(1) subject to a "Public Interest Override" (see section 8(2) of the Central Act). What this means is that even where requested information is covered by an exemption, the information should still be disclosed to the applicant if the public interest in the specific case requires it.

The NSG is a special forces unit under the Ministry of Home Affairs, and it may fall under the category of security and intelligence agencies which are generally exempt from the RTI Act, particularly when the information concerns matter of national security.

39 In India, the obligation to appoint a Grievance Officer applies ONLY to companies that?

* A. Deal with sensitive personal data.
* B. Conduct cross-border data transfers.
* C. Are considered part of the public sector.
* D. Lack alternate enforcement mechanisms.

According to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under the Information Technology Act, 2000, companies that collect, store, process, or handle sensitive personal data or information are required to appoint a Grievance Officer. The Grievance Officer is responsible for addressing complaints and ensuring compliance with the provisions of the IT Rules related to data protection.

Grievance Officers Required by IT Act 43A and Rule 5(9) Located at company dealing with SPI. Handles any discrepancies and grievances of the provider of info with respect to processing of information in a time bound manner. Must redress within one month.

Grievance Officers in companies (IT Act section 43A and rule 5(9)) Any company in India that deals with ‘sensitive personal information’ must ‘address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner’ and must appoint ‘a Grievance Officer who shall redress the grievances… `within one month’. A Grievance Officer is therefore the first tier of complaint handling in this system, one element of the role of a Data Protection Officer in proposals currently under consideration in the EU. There are limitations on the scope of the obligation: it applies only to companies that deal with ‘Sensitive Personal Data’, not any personal information; data subjects can only use the provision where they have provided the information to the company; and Grievance Officers need not deal with them in relation to personal information obtained from other sources.

Rule 5: Data Protection Principles (9) Complaint handling ♣ No obligation to address and respond to complaints. ♣ Company must designate Grievance Officer (and publish name and contact details on website), who must redress within 1 month.

40 Section 43A of India's IT Rules 2011 requires which of the following for a privacy policy?

A. It should be available and produced on request.

B. It should be published on the website of the body corporate.

C. It should be emailed or faxed to data providers by the body corporate.

D. It should be shown to the data provider at the time of data collection.

According to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under Section 43A, a body corporate must have a privacy policy for handling personal information and ensure that the policy is available and published on its website. This ensures transparency and accessibility for data providers regarding how their personal information is collected, used, and managed.

Answer B - Rule 4 imposes a duty on Body Corporates seeking sensitive personal data to draft a privacy policy and make it easily accessible for people who are providing the information. The privacy policy should be clearly published on the website of the body corporate and should contain details on the type of information that is being collected, the purpose for which it has been collected and the reasonable security practices that have been undertaken to maintain the confidentiality of such information.

41 All of the following are exempt from Section 43A of India's IT Rules 2011 EXCEPT?

* A. Charitable groups.
* B. Sole proprietorships.
* C. Government agencies.
* D. Religious organizations.

Section 43A of India's IT Rules 2011 applies to body corporates, which includes companies and other legal entities but not to individual entities like sole proprietorships. However, charitable groups, government agencies, and religious organizations are generally exempt from the provisions of Section 43A. Sole proprietorships are not specifically mentioned as exempt, meaning they could still fall under the scope of Section 43A if they engage in activities that involve handling sensitive personal data.

(i) Limitation to ‘body corporate’ and ‘commercial or professional activities. Section 43A - only APPLIES to a ‘body corporate’, which ‘means any company and includes a firm, SOLE PROPRIETORSHIP or other association of individuals engaged in commercial or professional activities. Religious and social organizations, including charities, whose activities are not classified as ‘Commercial’ will also be a substantial exclusion from the scope of the law. Although there are some public sector bodies which come within this, such as state-owned corporations, there is very limited coverage of the public sector.

All of India's right to information laws contained exemptions provisions. In the Central Act, section 8(1) lists all of the exemptions. Below is a general discussion of the exemption provisions: • National Security or Sovereignty: • National Economic Interests: • Relations with Foreign States: • Law Enforcement and the Judicial Process: • Cabinet and Other Decision-Making Documents: • Trade Secrets and Commercial Confidentiality: • Personal Privacy: • Individual Safety: It is extremely positive that the Central Act makes all of the exemptions contained in section 8(1) subject to a "Public Interest Override" (see section 8(2) of the Central Act). What this means is that even where requested information is covered by an exemption, the information should still be disclosed to the applicant if the public interest in the specific case requires it.

Only religious, social and charitable organisations and non-commercial organisations (such as government agencies) that do not engage in activities classified as "commercial" (hence not within the scope of "body corporate" in section 43A) are exempted from section 43A of the IT Act.

Only activities that are not classified as "commercial" are not within the scope of "body corporate" in section 43A and hence exempt from section 43A. Religious and social, charitable organisations and government agencies do not engage in commercial activities hence are exempt.

SCENARIO – Please use the following to answer the next question:  
Bharat Medicals is an established retail chain selling medical goods, with a presence in a number of cities throughout India. Their strategic partnership with major hospitals in these cities helped them capture an impressive market share over the years. However, with lifestyle and demographic shifts in India, the company saw a huge opportunity in door-to-door delivery of essential medical products. The need for such a service was confirmed by an independent consumer survey the firm conducted recently.  
The company has launched their e-commerce platform in three metro cities and plans to expand to the rest of the country in the future. Consumers need to register on the company website before they can make purchases. They are required to enter details such as name, age, address, telephone number, sex, date of birth and nationality – information that is stored on the company's servers. (Consumers also have the option of keeping their credit card number on file, so that it does not have to be entered every time they make payment.) If ordered items require a prescription, that authorization needs to be uploaded as well. The privacy notice explicitly requires that the consumer confirm that he or she is either the patient or has consent of the patient for uploading the health information. After creating a unique user ID and password, the consumer's registration will be confirmed through a text message sent to their listed mobile number.  
To remain focused on their core business, Bharat outsourced the packaging, product dispatch and delivery activities to a third-party firm, Maurya Logistics Ltd., with which it has a contractual agreement. It shares with Maurya Logistics the consumer name, address and other product-related details at the time of every purchase.  
If consumers underwent medical treatment at one of the partner hospitals and consented to having their data transferred, their order requirement will be sent to their Bharat Medicals account directly, thereby doing away with the need to manually place an order for the medications.  
Bharat Medicals takes regulatory compliance seriously; to ensure data privacy, it displays a privacy notice at the time of registration, and includes all the information that it collects. At this stage of their business, the company plans to store consumer information indefinitely, since the percentage of repeat customers and the frequency of orders per customer is still uncertain.

42 When collecting personal data, Bharat Medicals does NOT need to inform the consumer of what?

* A. The recipients of the collected data.
* B. The name of the body collecting the data.
* C. The type of safeguards protecting the data.
* D. The options the subject has to access his data.

According to India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, when collecting personal data, the organization must inform the data subject about the purpose of data collection, the intended recipients of the data, the name and address of the entity collecting and retaining the data, and the options available to the data subject to access and correct their data. However, it is not explicitly required to inform the consumer about the type of safeguards protecting the data.

5. Collection of information. — (3) While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the KNOWLEDGE of — (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information. (8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 80

A and B: Required under rule 5(3) C: Required under rule 4 (Provide privacy policy that states, inter alia, the reasonable security practices and procedures)

43 Which type of information collected by Bharat Medicals is considered sensitive personal information under the Information Technology Rules?

* A. Prescription details.
* B. Location data.
* C. Nationality.
* D. Religion.

Prescription details fall under the category of health information, which is considered sensitive personal data under the IT Rules. Sensitive personal data includes information such as passwords, financial information, health conditions, medical records and history, biometric information, and any detail related to physical, physiological, and mental health conditions.

Sensitive Personal Information (IN) IN– Password; financial info; physical, physiological, or mental health; sexual orientation; medical records and history; biometrics; any detail of the above as provided to a corporate entity for providing services; any of the info receive above for storing or processing under lawful contracts.

44 If a patient withdraws consent provided to one of the partner hospitals regarding the transfer of their data, which of the following would be true?

* A. The patient cannot purchase medications from Bharat Medicals.
* B. The hospital has the right to refuse withdrawal of consent since it has a partnership with Bharat Medicals.
* C. The hospital will obtain the necessary medications from Bharat Medicals and provide them directly to patient.
* D. The patient can buy medications from Bharat Medicals by uploading prescription to the Bharat Medicals website.

Even if the patient withdraws consent for the hospital to transfer their data directly to Bharat Medicals, they can still purchase medications from Bharat Medicals by manually uploading the necessary prescription information to the Bharat Medicals website. This ensures that the patient maintains control over their personal data while still being able to access the services provided by Bharat Medicals.

Patient may have withdrawn the consent provided to one of the partner hospitals regarding the transfer of their data - Bharat Medical’s e-commerce platform with door-to-door delivery facility and tie- up with strategic partnership with major hospitals in India, patient can upload the prescription along with authorization, because the consent with Bharat medicals is still valid

45 Which of the following is NOT true for Maurya Logistics?

* A. It must have a privacy policy on its website describing its data processing practices.
* B. It must obtain consent from Bharat Medicals consumers before processing their data.
* C. It must process Bharat Medicals' consumer data only according to agreed contractual terms.
* D. It must protect any unauthorized access any of Bharat Medicals consumer data that it obtained

As a third-party service provider, Maurya Logistics processes data on behalf of Bharat Medicals under the terms of their contractual agreement. The responsibility for obtaining consent from consumers lies with Bharat Medicals, not with Maurya Logistics. Maurya Logistics is required to process the data in accordance with the agreed contractual terms and ensure the data is protected from unauthorized access, but it does not need to obtain separate consent from the consumers.

Data subject consent Maurya Logistics is a processor and Bharat Medicals is a controller, the controller takes care of consent part. Maurya Logistics will be looking after the following functions - packaging, product dispatch and delivery Data Intermediary - The Data Intermediary is referred to differently depending upon the country or jurisdiction. In Singapore, it is data intermediary. In EU – the data processor, And in the United States / India – a data processor is typically referred to as a vendor, service provider or a third-party service provider.

46 In India's IT Rules 2011, which is included in the definition of "sensitive personal data"?

* A. Tax records.
* B. IP addresses.
* C. Next of kin.
* D. Sexual Orientation.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, define "sensitive personal data or information" to include details such as passwords, financial information, physical, physiological, and mental health conditions, sexual orientation, medical records and history, and biometric information.

3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Passwords, Financial information, physical or mental or physiological conditions, sexual orientation, medical records and history and biometric data provided that the information is not freely available/accessible in public domain or furnished under the Right to Information Act

47 What does NOT need to be considered when determining the retention schedule for sensitive personal data?

* A. Business needs.
* B. Amount of data.
* C. Storage capacity.
* D. Regulatory requirements.

When determining the retention schedule for sensitive personal data, the primary considerations should be business needs, the amount of data, and regulatory requirements. Storage capacity is not typically a key factor in determining how long sensitive personal data should be retained. Instead, the focus is on compliance with legal and regulatory obligations, ensuring data is kept only as long as necessary for business purposes, and minimizing risks associated with retaining large amounts of sensitive data.

1. The first consideration for data retention is always regulatory compliance (Regulatory requirements) 2. Organizational need with justification in the policy 3. Amount of data -not too much of something or not too little-Goldilocks

Storage capacity relates to the technical aspect of data management and does not directly impact the determination of retention schedules for sensitive personal data. However, the other options listed—business needs, amount of data, and regulatory requirements—are crucial factors to consider in establishing retention schedules for sensitive personal data

48 What benefit does making data pseudonymous offer to data controllers?

* A. It ensures that it is impossible to re-identify the data.
* B. It eliminates the responsibility to report data breaches.
* C. It allows for further use of the data for research purposes.
* D. It eliminates the need for a policy specifying data subject access rights.

Pseudonymisation helps protect individuals' identities by replacing identifiable information with pseudonyms, making it more challenging to link the data to specific individuals without additional information. This process facilitates the use of data for research and other purposes while providing a level of privacy protection. However, pseudonymisation does not make re-identification impossible, eliminate the responsibility to report data breaches, or remove the need for policies specifying data subject access rights.

Option A is wrong, Pseudonymization REDUCES the risk of re-identification not IMPOSSIBLE Anonymization and Pseudonymization: Anonymization and pseudonymization tools help protect personal data by removing or replacing identifying information, respectively. These techniques reduce the risk of re-identification and enhance data protection while allowing organizations to use data for analytical or research purposes.

Both A and C are correct. Pseudonymization helps to protect the privacy of individuals by replacing personally identifiable information with artificial identifiers, making it difficult to re-identify individuals directly. Also, by pseudonymizing the data, personally identifiable information is replaced with artificial identifiers, which reduces the risk of identifying individuals directly. This allows data controllers to use the data for various purposes, including research, while still protecting the privacy of individuals.

49 How is the transparency of the complaint process treated in both Hong Kong and Singapore?

* A. A complainant must alert all individuals potentially affected by the complaint.
* B. Investigations into complaints in Hong Kong and Singapore are open to the public.
* C. The Hong Kong and Singapore Commissioner may require the complainants to identify themselves before carrying out any investigation into the complaint.
* D. The Hong Kong and Singapore commissioners are obliged to start investigations when receiving a complaint and inform the respondent of the personal details of the complainant.

Both jurisdictions have mechanisms in place to handle complaints regarding data privacy, and the commissioners may require complainants to provide their identities to prevent frivolous or anonymous complaints. This ensures that the complaint process is conducted with accountability and that legitimate concerns are addressed appropriately. However, the investigations are not necessarily open to the public, and the commissioners are not obliged to start investigations in all cases upon receiving a complaint.

Hong kong… Section 39: (1) Notwithstanding the generality of the powers conferred on the Commissioner by this Ordinance, the Commissioner may refuse to carry out or decide to terminate an investigation initiated by a complaint if – Section 39: (1) (b) the complaint is made anonymously; (c) the complainant cannot be identified or traced; Singapore… An individual may lodge a complaint relating to personal data protection to the PDPC. Under the PDPA, only individuals who have suffered loss or damage directly as a result of a contravention Personal Data Protection Complaint Please have your Singpass ID and password ready to submit a complaint to the PDPC. Officers may contact you via email or telephone if any clarification is required.

SCENARIO – Please use the following to answer the next question:  
Dracarys Inc. is a large multinational company with headquarters in Seattle, Washington, U.S.A. Dracarys began as a small company making and selling women's clothing, but rapidly grew through its early innovative use of online platforms to sell its products. Dracarys is now one of the biggest names in the industry, and employs staff across the globe, and in Asia has employees located in both Singapore and Hong Kong.  
Due to recent management restructuring they have decided, on the advice of external consultants, to open an office in India in order to centralize its call center as well as its internal human resource functions for the Asia region. Dracarys would like to centralize the following human resource functions in India:  
1. The recruitment process;  
2. Employee assessment and records management;  
3. Employee benefits administration, including health insurance.  
Dracarys will have employees on the ground in India managing the systems for the functions listed above. They have been presented with a variety of vendor options for these systems, and are currently assessing the suitability of these vendors for their needs.  
The CEO of Dracarys is concerned about the behavior of her employees, especially online. After having proprietary company information being shared with competitors by former employees, she is eager to put certain measures in place to ensure that the activities of her employees, while on Dracarys' premises or when using any of Dracarys' computers and networks are not detrimental to the business.  
Dracarys' external consultants are also advising the company on how to increase earnings. Dracary's management refuses to reduce production costs and compromise the quality of their garments, so the consultants suggested utilizing customer data to create targeted advertising and thus increase sales.

50 Dracary's existing client data sets have been anonymised but the CEO is concerned about re-identification and the risks of using the data for further analysis.  
What should the CEO do?

* A. Assess the business risk of further processing in the absence of any regulations on anonymised data.
* B. Refer to India's Information Technology Act and the 2011 rules 3-8 for guidance on handling anonymised data.
* C. Obtain the consent of the data subjects because anonymous data must be treated as personal data at all times.
* D. Adhere to the Singapore guidelines on anonymization and the Hong Kong Guidance on Personal Data Erasure and Anonymization.

While India's Information Technology Act and the 2011 rules provide some guidance on data protection, they may not specifically address anonymized data. Since Dracarys has employees and operations in both Singapore and Hong Kong, it is prudent to follow the data protection guidelines of these jurisdictions, especially concerning anonymization and the re-identification of anonymized data.

Adhering to the Singapore guidelines and Hong Kong Guidance will help ensure that Dracarys remains compliant with relevant data protection regulations in these jurisdictions and manages the risks associated with further processing anonymized data. Additionally, these guidelines will provide a comprehensive approach to handling anonymized data and help mitigate potential risks of re-identification.

The answer is there in option A – “in the absence of any regulations on anonymized data “ D. Adhere to the Singapore guidelines on anonymization and the Hong Kong Guidance on Personal Data Erasure and Anonymization. Since, Singapore and Hong Kong, PCPD, and PDPA – both have regulations and guidelines on Anonymization.

51 Which of the following guidelines does Dracarys NOT need to take into account when implementing monitoring and surveillance tools?

* A. The Indian Information Technology Act of 2000.
* B. The Hong Kong guide to monitoring personal data privacy at work.
* C. The Hong Kong Code of Practice on Human Resource Management.
* D. The Singapore advisory guidelines on the personal data protection act for selected topics (employment and CCTV).

The Hong Kong Code of Practice on Human Resource Management is specific to human resource practices and data privacy in the context of employment within Hong Kong. While it provides valuable guidance on managing employee data, it is not directly relevant to implementing monitoring and surveillance tools for employees in India.

However, Dracarys should consider the following guidelines:

A. The Indian Information Technology Act of 2000: This Act, along with its associated rules, provides the legal framework for data protection and privacy in India, which is crucial for implementing any monitoring tools.

B. The Hong Kong guide to monitoring personal data privacy at work: While this guide is specific to Hong Kong, it provides best practices and principles for monitoring personal data privacy at work, which could be useful for developing ethical and compliant monitoring practices.

D. The Singapore advisory guidelines on the personal data protection act for selected topics (employment and CCTV): These guidelines offer valuable insights into the principles and practices for employee monitoring and the use of CCTV, which can help ensure compliance with data protection laws and respect for privacy.

A, as it is the only one of the options without any specific mentions of employee surveillance and monitoring.

52 What must Dracarys confirm about the vendor in India in order to centralize elements of its Human Resource function?

* A. That the vendor submits for approval from Dracarys a privacy notice explaining how personal data will be protected under the Indian Information Technology Act.
* B. That the vendor files requests for transfer of personal data out of India through the offices of the privacy commissioners of Hong Kong and Singapore.
* C. That the vendor is bound by legally enforceable obligations to provide the personal data a standard of protection that is at least comparable to the protection under the Singapore PDPA.
* D. That the vendor adheres to the same sector privacy rules followed by Dracarys headquarters based in Seattle regarding the transfer of personal data.

Ensuring that the vendor in India is legally obligated to protect personal data to a standard comparable to Singapore's Personal Data Protection Act (PDPA) is crucial. This ensures that personal data of employees, especially from Singapore, will be adequately protected and compliant with Singapore's data protection laws, even when processed in another country. This approach helps mitigate risks associated with cross-border data transfers and ensures consistency in data protection standards.

A - So as to meet the requirement under Rule 8, i.e. that reasonable security practice and procedures be maintained. This requirement can be met by meeting an industry standard or code of practice.

53 Dracarys and their vendor of choice must draft a contract that establishes agreement regarding all of the following factors EXCEPT?

* A. Breach notification.
* B. Data retention periods.
* C. Employee recruitment process.
* D. Data subject consent provisions.

While the employee recruitment process is an important function being centralized, it is not typically a factor that needs to be explicitly detailed in a contract between Dracarys and the vendor regarding data protection and privacy. The focus of the contract should be on data protection aspects such as breach notification, data retention periods, and data subject consent provisions to ensure compliance with relevant data protection laws and the safeguarding of personal data.

D - Data subject consent provisions Vendor is a processor and Dracarys is a controller, the controller takes care of consent. Vendor will be looking after the following functions and their privacy policy must be aligned with Dracarys… Human resource functions in India: 1. The recruitment process; 2. Employee assessment and records management; 3. Employee benefits administration, including health insurance. Data Intermediary - The DI is referred to differently depending upon the country or jurisdiction. In Singapore, it is data intermediary. in EU – the data processor, And in the United States – a data processor is typically referred to as a vendor, service provider or a third-party service provider.

Answer is D, because data subject consent, if required, should be obtained by Dracarys Inc and not the vendor.

54 How are the scope of Singapore's Personal Data Protection Act and the scope of India's IT Rules similar?

* A. They only apply to the private sector.
* B. They allow exemptions for military personnel.
* C. They apply to controllers and processors alike.
* D. They impose obligations on individuals acting in a domestic capacity.

Both Singapore's PDPA and India's IT Rules primarily regulate the processing of personal data by private sector organizations. They do not generally apply to government agencies or public sector entities and focus on the responsibilities and obligations of private organizations in handling personal data.

Scope of the PDPA The PDPA covers personal data stored in electronic and non-electronic formats. It generally does not apply to: Any individual acting on a personal or domestic basis. Any individual acting in his/her capacity as an employee with an organisation. Any public agency in relation to the collection, use or disclosure of personal data. 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. Who does Singapore PDPA apply to? The PDPA's main data protection obligations apply to all private sector organizations in Singapore, regardless of size, if they collect, use, or disclose the personal data of Singaporeans. It doesn't impose obligations on: Individuals in personal or domestic capacities. The Information Technology Amendment Act is applicable to any person, company or organization that uses computer systems, computer networks or other information technology in India.

55 Both Sections 72 and 72A of India's IT Act 2000 involve unauthorized access of personal information. One main difference between the sections is that 72A does what?

* A. Stipulates that disclosure has to have occurred.
* B. Specifies imprisonment as a possible penalty.
* C. Adds a provision about wrongful loss or gain.
* D. Includes the concept of consent.

Section 72 deals with unauthorized access and disclosure of information by someone who has secured access through the lawful power of the government. In contrast, Section 72A specifically addresses unauthorized access and disclosure by service providers and includes provisions that the disclosure must have caused wrongful loss or gain.

Section 72A: “Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract Both 72 and 72A Specify imprisonment

56 In 2013-14, the Indian Supreme Court ruled in Puttaswamy and Anr. vs Union of India that requiring a Unique Identification Number was unconstitutional if what?

* A. It was restricted to residents of India.
* B. It was necessary for proving citizenship.
* C. It was required in order to obtain government services.
* D. It was used to gather information to discriminate against minorities.

The Supreme Court of India held that the Aadhaar (Unique Identification Number) could not be made mandatory for accessing government services, as it would infringe on individuals' rights to privacy and could potentially deny citizens access to essential services if they did not have the number.

57 Which of the following topics was NOT addressed in India's Information Technology Act 2000 (IT Act)?

* A. Digital signatures.
* B. Censorship limitations.
* C. Electronic transactions.
* D. Cybersecurity procedures.

The IT Act primarily focuses on digital signatures, electronic transactions, and cybersecurity procedures. It aims to provide a legal framework for electronic commerce and to address issues related to cybercrime and electronic data protection. Censorship limitations are not a primary focus of the IT Act.

Information Technology Act, 2000 Provide legal recognition to electronic records and digital signatures: The Act aims to give legal validity and enforceability to 1. Electronic records 2. And digital signatures at par with physical documents and handwritten signatures. 3. cybercrime and e-commerce This enables e-governance and e-commerce. In accordance with A 19(2), the IT Act contains numerous provisions that can be used to censor online content – notably in Sections 66A, 69A and 79. Most tellingly almost all these instances involve executive action with no system of judicial oversight – in fact under Section 79, the law actively encourages private censorship.

Should be B. The Information Technology Act 2000 (IT Act) primarily focuses on issues such as digital signatures, electronic transactions, and cybersecurity procedures. However, censorship limitations are not a central focus of this legislation.

58 In addition to adhering to the data export principle of section 43A of India's IT Act 2000, data exporters in India must also follow principles of?

* A. Privity of contract.
* B. Disclosure limitation.
* C. Mandatory registration.
* D. Third party assessment.

Section 43A of India's IT Act 2000, along with the associated rules, emphasizes the need for organizations to implement reasonable security practices and procedures to protect sensitive personal data or information. Disclosure limitation is a key principle, ensuring that personal data is only disclosed to third parties for purposes consistent with the consent given by the data subjects and within the scope of the original data collection purpose.

Section 43A and the 2011 Rules 3-8 Rule 6: Disclosure Limitations and Exceptions ♣ SPI only: Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation. ♣ Companies prohibited from “publishing” SPI. ♣ Third parties receiving SPI shall not disclose it further. ♣ EXCEPTION: Disclosure permitted to govt agencies mandated by law to obtain info (including SPI) for verification of ID, prevention, detection, investigation of cyber incidents, prosecution, punishment. ♣ No disclosure rights for data subject if data subject is not also provider.

Disclosure limitations and exceptions (rule 6) Companies disclosing ‘sensitive personal data or information’ to any third party require prior permission from the provider of the personal data who has provided such information under lawful contract or otherwise to the body corporate. Disclosures agreed by contract between the provider of the information, or necessary for compliance with a legal obligation, are also allowed. Companies must not ‘publish’ sensitive personal information (presumably meaning they must not make it generally available to the public). Third parties receiving sensitive personal data under this Rule ‘shall not disclose it further’.

Should be B - disclosure limitation. Disclosure limitation (Rule 6 of the IT rules) is an essential aspect of data protection and privacy regulations. It involves restricting the amount of sensitive information that can be accessed or disclosed to third parties without proper authorization. This principle is particularly important in the context of data export to ensure that personal data is adequately protected during transfer.

59 Which European-influenced safeguard was NOT included in Hong Kong or Singapore's personal data protection acts, but was subsequently adopted as a consideration in regulatory guidelines?

* A. Controls on automated decision making.
* B. Additional protection for sensitive personal data.
* C. Legitimate interest as a legal basis for processing.
* D. Notice requirements when data is collected from third parties.

While Hong Kong and Singapore's personal data protection laws initially did not include specific controls on automated decision making similar to those in the European Union's General Data Protection Regulation (GDPR), such considerations have been recognized and addressed in subsequent regulatory guidelines to ensure that individuals' rights are protected in the context of automated processing and decision-making.

Singapore Personal Data Protection Commission (“PDPC”) has issued its first decision on the Legitimate Interests Exception under the PDPA. While the PDPA remains largely a consent-based regime, the Legitimate Interests Exception is one of the exceptions from consent available under the PDPA. Yes, the PCPD confirmed that there is a legitimate basis for employers to collect additional data of the subjects.

60 Under India's IT Rules 2011, data subjects have the right to correct inaccuracies in personal information collected about them only if?

* A. They are also the providers of the information.
* B. They confirm their consent to maintain the information.
* C. They are able to prove the legitimacy of the corrections.
* D. They request the corrections within a specified amount of time.

The IT Rules provide that the body corporate or any person who on behalf of the body corporate collects, receives, possesses, stores, deals, or handles information shall permit the providers of the information to review the information they have provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient is corrected or amended as feasible.

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible: Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by

Should be C. Data subjects have the right to correct inaccuracies in personal information collected about them, but they must be able to provide legitimate proof for the corrections. This means that individuals must provide evidence supporting the accuracy of the corrections they wish to make to their personal information.

61 Which was NOT listed as an individual right in the 1998 Fair Information Practice Principles (FIPPs)?

* A. Notice.
* B. Choice.
* C. Right to erasure.
* D. Right to data access.

The 1998 FIPPs, established by the U.S. Federal Trade Commission (FTC), included principles such as Notice, Choice, Access, and Security. The Right to Erasure, which allows individuals to request the deletion of their personal data, was not included in the original FIPPs but is a concept that has gained prominence in more recent privacy regulations like the EU's General Data Protection Regulation (GDPR).

APEC information privacy principles 1. Preventing Harm 2. Notice 3. Collection Limitations 4. Uses of Personal Information 5. Choice 6. Integrity of Personal Information 7. Security Safeguards 8. Access and Correction 9. Accountability

Should be C. The 5 principles are (1)notice/awareness (2) choice/consent (3) access/participation (4) Integrity/security and (5) enforcement/redress. Right to erasure is not one of the fair principles of the US Fair Information Practices

62 Which of the following countries will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary?

* A. Argentina.
* B. Mexico.
* C. Taiwan.
* D. Korea.

Argentina is one of the countries that has been granted adequacy status by the European Commission, meaning that its data protection laws are considered to provide a level of protection that is essentially equivalent to that provided by the GDPR. This status allows for the free flow of personal data from the EU to Argentina without the need for additional safeguards.

63 Under the General Data Protection Regulation (GDPR), European Union member states may be allowed to transfer personal data to the United States in some cases.  
Which of the following could NOT be used as a legitimate means of doing this?

* A. A consent derogation.
* B. A certification mechanism.
* C. Privacy Shield.
* D. Ad-hoc contractual clauses.

The EU-U.S. Privacy Shield framework was invalidated by the Court of Justice of the European Union (CJEU) in the Schrems II decision in July 2020. As a result, it is no longer a valid mechanism for transferring personal data from the EU to the U.S. However, other mechanisms such as consent derogation, certification mechanisms, and ad-hoc contractual clauses can still be used, provided they meet the specific requirements set out in the GDPR.

The Privacy Shield was a mechanism that was invalidated by the Court of Justice of the European Union in 2020, and therefore, it cannot be used as a legitimate means of transferring personal data to the United States under the GDPR. Therefore, option C is the correct answer to the question.

64 Which personal data element is NOT considered a special category of data under the General Data Protection Regulation (GDPR)?

* A. Physical or mental health data.
* B. Financial information.
* C. Race or ethnic origin.
* D. Political opinions.

Answer - B The following personal data is considered ‘sensitive’ and is subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person’s sex life or sexual orientation.

65 Which of the following is NOT a way that the Singapore government can monitor its citizens?

* A. Through the national identity card system.
* B. Through the electronic road pricing system.
* C. Through a personal computer registration system.
* D. Through an online service that holds an individual’s medical records.

Should be C. A is the Singapore's NRIC system. B is the ERP system. D is the national online system for holding patient records from hospitals and clinics in Singapore.

66 What was the basis for the "TrustSg" mark, which was designed to build confidence in e-commerce transactions before the PDPA was enacted?

* A. The Fair Information Practice Principles.
* B. The Model Data Protection Code.
* C. The Electronic Transactions Act.
* D. The 1995 European Directive.

The gestation(the development of ‘TrustSg’ over a period of time) of the law is traced by Chesterman, commencing with a ‘Model Code’ of 10 principles, developed by Singapore’s National Internet Advisory Committee. ‘Model Code’ subsequently became the basis for the ‘TrustSg’ trustmark administered by Singapore’s National Trust Council, a system ‘not regarded as particularly effective’, although some revocations of trustmarks have occurred.

The basis for the "TrustSg" mark, which was designed to build confidence in e-commerce transactions before the Personal Data Protection Act (PDPA) was enacted. The "TrustSg" mark was developed under the framework of the Electronic Transactions Act to establish a trusted environment for electronic commerce in Singapore. It aimed to provide assurance to consumers about the reliability and integrity of e-commerce transactions, thereby fostering trust in online business activities.

67 What emerged as the main reason for creating a comprehensive data protection law when Singapore ministers met between 2005 and 2011?

* A. To control increasing technological threats.
* B. To raise Singapore's human rights standing.
* C. To limit the scope of governmental surveillance.
* D. To enhance Singapore's economic competitiveness

The PDPA’s origins Singapore is one of the last economically advanced countries to adopt a COMPREHENSIVE DATA PRIVACY LAW for its private sector. The gestation of the law is traced by Chesterman. It subsequently became the basis for the ‘TrustSg’ trustmark administered by Singapore’s National Trust Council, a system ‘not regarded as particularly effective’, although some revocations of trustmarks have occurred. An inter-Ministry committee started to consider data protection legislation in 2005, and proceeded through a series of overseas investigations, consultation papers, and submission rounds.

Chesterman sees the primary motivations for the Singapore legislation as ECONOMIC An inter-Ministry committee started to consider data protection legislation in 2005, and proceeded through a series of overseas investigations, consultation papers, and submission rounds. The PDPA which emerged from the process is in most respects the same as the draft Bill announced earlier in 2012 by the then Ministry of Information, Communications and the Arts, which confirmed many features foreshadowed in a previous discussion paper. However, other features were jettisoned, generally resulting in improved privacy protections. Chesterman sees the primary motivations for the Singapore legislation as ECONOMIC, rather than civil liberties or consumer protection, concerns which aim to increase the flow of personal data into Singapore by making it become a ‘trusted node’. Whether the Act will or should succeed in creating such international trust is arguable、

One of the purposes of the PDPA is to “increase consumer trust and strengthen Singapore's position as a trusted global data hub.”

The motivation behind enacting the Personal Data Protection Act (PDPA) was primarily to boost Singapore's reputation as a trusted hub for businesses, thereby enhancing its economic competitiveness. The comprehensive data protection law aimed to foster consumer trust in businesses handling personal data, which is crucial for the growth of the digital economy and attracting international business operations.

68 Which of the following is NOT excluded from the scope of Singapore's Do Not Call registry?

* A. Messages that promote investment opportunities.
* B. Messages that conduct market research.
* C. Messages from charitable organizations.
* D. Messages from political candidates.

The marketing messages covered under DNC provisions include voice calls, text or fax messages, for the purposes of: Offering to supply, advertise or promote goods or services; Advertising/promoting suppliers or prospective suppliers of goods or services; or Supplying/advertising/promoting land, interests in land or business/investment opportunities. Whether your organisation is directly sending such marketing messages, causing the message to be sent or authorising another organisation to do so, you have to ensure that such messages are not sent to Singapore telephone numbers registered with the DNC Registry.

Exceptions You do not need to check the DNC Registry if your organisation has the recipient’s clear and unambiguous consent to send marketing messages to the Singapore telephone number. Additionally, you may send: Voice calls, text or fax messages about products, services and memberships that are relevant to individuals with whom your organisation has an ongoing relationship (note: a series of one-off transactions does not constitute an ongoing relationship); Service calls or reminder messages regarding services bought by the individual; Messages as part of a market survey or research; Messages relating to charitable or religious causes; or Messages targeting businesses (i.e. B2B) and not individuals.

option A is missing from the DNC registry... Do note that the DNC Registry does not cover: Marketing messages or calls from organisations with whom you have an ongoing relationship, if the messages are about products or services that are relevant to you. However, you may opt out from receiving such telemarketing messages and the organisation must stop sending such messages to your Singapore telephone number after 21 calendar days; Messages that are part of a market survey or research; Messages related to charitable or religious causes; Personal messages sent by individuals; Public messages sent by government agencies; Political messages; or Telemarketing calls or messages sent to a BUSINESS (i.e. B2B).

B2C marketing messages such as those that promote investment opportunities are precisely the type of messages that is include in the scope of the DNC Registry.

69 In what case would a foreign company NOT be liable for breaches of Singapore's PDPA?

* A. If it has a physical office in Singapore.
* B. If it is storing information in Singapore.
* C. If it is collecting personal information in Singapore.
* D. If it collects information from Singaporeans living abroad.

The Act has an extraterritorial effect, meaning it applies to organizations collecting, using or disclosing personal data in Singapore whether or not the organization itself has a physical presence or is registered as a company in Singapore. The PDPA applies to organisations collecting, using, and disclosing personal data in Singapore, whether or not formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore. Organisation' is defined in the PDPA 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.'

70 In enforcement cases, what is Singapore's Personal Data Protection Commission (PDPC) obligated to do?

* A. Publish the decisions it makes regarding complaints.
* B. Provide the complainant with a way to appeal a decision.
* C. Publish the name of an organization named in a complaint.
* D. Intervene in civil actions to provide assistance to complainants.

The PDPC publishes its enforcement decisions to maintain transparency and provide guidance to organizations and the public on the interpretation and application of the Personal Data Protection Act (PDPA). This practice helps in setting precedents and educating stakeholders on compliance requirements.

The other options are not obligations of the PDPC:

B. Provide the complainant with a way to appeal a decision: While there may be avenues for appeal, it is not specifically stated as an obligation for the PDPC to provide this.

C. Publish the name of an organization named in a complaint: The PDPC may choose to do this in certain cases, but it is not obligated to publish the names of organizations in every instance.

D. Intervene in civil actions to provide assistance to complainants: The PDPC's role is regulatory and enforcement-related, not to intervene in private civil actions.

71 Protection of which kind of personal information is NOT explicitly mentioned in the privacy laws of Hong Kong, Singapore, and India?

* A. Sensitive data.
* B. Children's data.
* C. Outsourced data.
* D. Extraterritorial data.

The protection of children's data is NOT explicitly mentioned in the privacy laws of Hong Kong, Singapore, and India.

Here's a breakdown:

Sensitive data: All three jurisdictions have provisions for the protection of sensitive personal data, although the specifics may vary.

Outsourced data: Privacy laws in these countries typically address data protection responsibilities when data is outsourced to third parties.

Extraterritorial data: The privacy laws may include provisions that apply to data collected or processed outside their borders but related to their citizens or residents.

However, specific protections for children's data, such as age-based consent requirements or specific regulations targeting the collection and use of data from minors, are not explicitly and comprehensively covered in the privacy laws of Hong Kong, Singapore, and India. While there may be some general protections that apply, there is not a specific, detailed focus on children's data comparable to frameworks like the Children's Online Privacy Protection Act (COPPA) in the United States or similar regulations in other jurisdictions.

Outsourced Data India amendments were brought in the information Technology Act, 2000 to provide the measures for data protection in India which may assuage the fears of misuse of data / information being dealt with by the outsourcing industry or the IT Sector or during the e-commerce for the time being.. Hongkong The Personal Data (Privacy) (Amendment) Ordinance 2012 provides enhanced protection in this respect by introducing, with effect from 1 October 2012, additional obligations on data users to use contractual or other means to monitor their data processors' compliance with data protection requirements. Singapore the relevant obligations under the Personal Data Protection Act (PDPA) and key considerations for organisations (i.e., Data Controllers) which outsource data processing activities to other entities (i.e., Data Intermediaries). Data Controllers (DC) that ensure accountability1 through their management of Data Intermediaries (DI) provide greater assurance for customers and enhance their business

Children's data India Section 9 of the PDPA specifically deals with the processing of the personal data of a child. It states that before any such processing takes place, verifiable consent needs to be taken from the parent of the child. Hongkong The Special Needs of Children Children are often identified as a vulnerable group who have special requirements in privacy protection, particularly in the context of online activities. When interacting with children, data users should bear in mind children’s vulnerability and consider adopting the following age-appropriate approaches to make sure that they protect and respect children’s personal data. Singapore's Personal Data Protection Commission released an advisory guide on how to comply with the children's privacy rules in the Personal Data Protection Act of 2012.

Extraterritorial effect SINGAPORE The Act has extraterritorial effect, meaning it applies to organizations collecting, using or disclosing personal data in Singapore whether or not the organization itself has a physical presence or is registered as a company in Singapore. India While the DPDP Act is applicable to Indian entities which engage in the processing of personal data, it also has extra-territorial applicability, applying to foreign entities who offer goods and services to Data Principals (as defined below) located within the territory of India and process personal data in connection to such activities. Hongkong The PDPO does not have extraterritorial effect and only applies to data users who control the collection, holding, processing or use of PI

Should be D. Extraterritorial data refers to data that is stored or processed outside the jurisdiction where the privacy laws apply. These laws often focus on data within their own territorial boundaries rather than data stored or processed abroad. Therefore, the protection of extraterritorial data is not explicitly mentioned in the privacy laws of these countries.

72 On what group does Singapore's PDPA impose disclosure restrictions that Hong Kong and India do not?

* A. Government officials.
* B. Children under 13.
* C. The deceased.
* D. The clergy.

Singapore's PDPA includes provisions regarding the protection of personal data of individuals who have passed away. This is a distinctive aspect of the PDPA, as neither Hong Kong nor India explicitly imposes such restrictions in their respective data protection laws.

Personal data of deceased individuals As noted earlier, the term “individual” includes both living and deceased individuals. Hence, the provisions of the PDPA will apply to protect the personal data of deceased individuals to the extent provided in the PDPA Specifically, the PDPA provides that the obligations relating to the disclosure and protection of personal data will apply in respect of the personal data about an individual who has been dead 10 years or less

The above obligations will apply in respect of the personal data of a deceased individual for 10 years from the date of death. This is intended to minimise any adverse impact of unauthorised disclosure of such data on family members of the deceased. Organisations should note that while the PDPA does not apply to personal data of individuals who have been deceased for more than 10 years, there may still be other legal or contractual requirements that organisations should be mindful of.

Should be C. Singapore's data protection laws covers personal data of the deceased (up to 10 years protection) while India and Hong Kong's do not.

73 In 2015, Section 66A of India's IT Act was ruled unconstitutional. What did this section previously prohibit?

* A. Publishing images with sexually explicit content.
* B. Tampering with computer source documents.
* C. Publishing private images of others.
* D. Sending offensive messages.

Section 66A and its Removal Became law in October 2009. Prohibited using computer or other communication device to send information that was grossly offensive, menacing, known to be false but for the purpose of annoying, insult, hatred, etc. Prohibited email with fake addresses. 3 years prison + fine. Supreme Court ruled section 66a to be entirely unconstitutional in 2015. Violated freedom of expression and speech. Freedom of expression cannot be suppressed unless the situations created by allowing the freedom are pressing and the community interest is endangered – and not a remote danger. Section 66A goes beyond defamation – something may be grossly offensive or annoying without being defamatory. Void for vagueness. Terms undefined. E.g. what is offensive to one person is not to another. Chilling effect on discussion of governmental, literary, scientific, etc.

No Person Should Be Prosecuted Under Section 66A IT Act : Supreme Court Issues Directions To Enforce Shreya Singhal Judgment The court struck down the provision as unconstitutional and a violation of free speech in 2015 in the Shreya Singhal Case. The section relating to restrictions on online speech was declared unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the Constitution of India

74 What clarifications did India make in a 2011 Press Note regarding their Sensitive Personal Data Rules?

* A. That the rules apply to data subjects located outside of India.
* B. That the rules apply to persons or companies collecting sensitive data within India.
* C. That the data processor must provide notice to the data subject before data is processed.
* D. That sensitive personal data or information includes passwords, financial information, medical records, and biometric information.

The 2011 Press Note was issued to provide clarification on the applicability of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. It specifically clarified that these rules are applicable to body corporates, or any person located within India that collects, receives, possesses, stores, deals, or handles sensitive personal data or information.

The Government of India Issues Clarifications to Its Data Privacy Rules September 9, 2011 On August 24, 2011, the Ministry of Communications and Information Technology of the Government of India ("IT Ministry"), through the Press Information Bureau, issued a press note ("Press Note") containing certain clarifications to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Privacy Rules") issued earlier in the year[1]. Most significantly, foreign companies are now excluded from the ambit of the obligations imposed by the Data Privacy Rules. Additionally, the scope of the Data Privacy Rules has been narrowed down with respect to Indian companies. Press Note Clarifications The Press Note clarifies certain provisions of the Data Privacy Rules, which include: Indian Companies Only: The obligations under the Data Privacy Rules apply only to Indian companies. Foreign companies are exempt.

75 Although the right to privacy is not explicitly granted in the Indian Constitution, privacy advocates frequently cite Article 21's guarantee of?

* A. Personal liberty.
* B. Right to property.
* C. Equality before the law.
* D. Freedom from intrusion.

Option A - Constitutional Protections Article 21 “No person shall be deprived of his life or personal liberty except according to procedure established by law.” - Interpreted by SC to include implied protection of privacy as essential ingredient of personal liberty. - Available to anybody, not just citizens. Option B - Right to Property was a Fundamental Right as per the Constitution of India till an amendment was done in 1978. This was the 44th amendment of the Constitution, Article 31 and Article 19(1)(f) was completely removed from the Part III – Fundamental Rights of Constitution. Option C - Article 14 – equality before law. Option D - red herring

The Supreme Court of India considered the citizen's right to privacy on a number of decision under Article 21 of the Constitution 1949, which provides that "No person shall be deprived of his or her life or personal liberty except according to the procedure established by law.

76 Which method ensures the greatest security when erasing data that is no longer needed, according to the Hong Kong Office of the Privacy Commissioner?

* A. Strip-shredding paper copies of data.
* B. Crosscut shredding paper copies of data.
* C. Deleting electronic files containing data.
* D. Reformatting USB memory devices containing data.

Crosscut shredding is more secure than strip-shredding because it cuts the paper into smaller pieces, making it much more difficult to reconstruct the original document. For electronic files, simply deleting or reformatting may not be sufficient, as the data can often be recovered using specialized software. Proper destruction of electronic data typically requires methods like overwriting, degaussing, or physically destroying the storage media.

Legal Requirements related to Personal Data Erasure Section 26 of the Ordinance provides that a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased. Safe and Secure Erasure Guidelines, and in some cases, procedures, should be established on the erasure method to be used for each type of records. The purpose of the erasure is to irreversibly delete or destroy the personal data so that it cannot be recovered. The method used must, therefore, match with the type of storage technology. For example, in the case of paper records, cross-cut shredding should be used instead of strip shredding so that individual sheets cannot be easily reconstructed.

See page 2 of the guidance of personal data erasure and anonymisation, issued by the HK office of the privacy commissioner.

77 In Hong Kong, which of the following are exempt from personal data access requests until after the project to which the data is related has been concluded?

* A. Hospital administrators.
* B. Financial institutions.
* C. News organizations.
* D. Non-profit groups.

Under the Personal Data (Privacy) Ordinance (PDPO) in Hong Kong, news organizations are exempt from certain obligations regarding personal data access requests while they are working on journalistic projects. This exemption is in place to protect the integrity and confidentiality of journalistic activities until the related project has been concluded.

Under section 61, if personal data is held for the purpose of news activities, such data may be exempt from the provision in respect of data-access requests under DPP 6 and sections 18(1)(b) and 38(i) unless and until the data is published or broadcast; and sections 36 and 38(b) of the Ordinance. If the data user has reasonable grounds to believe that the disclosure of the personal data is in the public interest, then such disclosure may also be exempt from the restrictions on use (DPP 3).

78 Under the PDPO, what are Hong Kong companies that make use of personal data required to do?

* A. Appoint an official compliance officer.
* B. Register with the appropriate data authority.
* C. Honor all data subject requests for correcting personal information.
* D. Provide contact information of persons handling data access requests.

The Personal Data (Privacy) Ordinance (PDPO) mandates that data users (companies) must allow individuals to access and correct their personal data. This means that companies must have procedures in place to handle and honor requests from data subjects to correct any inaccuracies in their personal information.

HONG KONG Currently, there is no legal requirement for data users to appoint a data protection officer in Hong Kong. Currently, there is no requirement for organizations that control the collection and use of personal data (known as "data users") to register with the data protection authority. Option D - it doesn't make sense, usually, the DPO's contact information is shared... Article 37(7) of the EU General Data Protection Regulation requires that “the controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.” The duties of a Data Protection Officer include: Working towards the compliance with all relevant data protection laws, monitoring specific processes, such as data protection impact assessments or the awareness SINGAPORE It is mandatory for each organization to appoint one or more DPOs to be responsible for ensuring the organization’s compliance with the Act There are no registration requirements under the Act.

79 Who is NOT potentially liable when an employee in a Singapore corporation or partnership breaches the PDPA?

* A. A corporate officer responsible of setting up data processing.
* B. The employee following the management processes.
* C. The employee’s direct manager overseeing data handling.
* D. A partner of the partnership handling data related matters

While employees can be held liable for personal actions, if they are acting strictly according to the management processes and policies set by their employer, the primary liability typically falls on the organization, the corporate officers, or managers responsible for setting up or overseeing data processing and handling. In contrast, employees who are simply following these established processes without deviation are generally not held individually liable.

Personal liability of corporate officers for offences The Act imposes personal liability on company officers for offences, an unusual provision in a data protection law: ‘Where an offence under this Act committed by a body corporate is proved — (a) to have been committed with the consent or connivance of an officer; or (b) to be attributable to any neglect on his part, the officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly’ (s52(1)) Personal and vicarious liabilities Singapore’s Act raises important issues for businesses trading in Singapore concerning who is liable for breaches and offences. Liability of employers - Any act done or conduct engaged in by an employee in the course of his or her "employment shall be treated as done or engaged in by the employer as well, whether or not it was with the employer's" knowledge or approval

Excluded organisations - The PDPA provides that the Data Protection Provisions do not impose any obligations on the following entities. These categories of organisations are therefore excluded from the application of the Data Protection Provisions: 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; and c) Any public agency Individuals acting as employees The second significant exclusion for individuals in the PDPA relates to employees who are acting in the course of their employment with an organisation. Employees are excluded from the application of the Data Protection Provisions. The PDPA defines an employee to include a volunteer. Hence, individuals who undertake work without an expectation of payment would fall within the exclusion for employees.

Case - Michael Reed vs Alex Bellingham vs Attorney-General ( Judith Prakash JCA -delivering the judgment of the court) Application of Act 4.—(1) Parts 3, 4, 5, 6, 6A and 6B do not impose any obligation on — (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. On this point, the appellant supports the Judge’s holding. In his submissions, the appellant accepts that if s 4(1)(b) of the PDPA applies, the respondent is not liable for any breach of ss 13 and 18 committed in the course of his employment. The liability would be that of the person who employed the respondent when he committed the breaches.

Should be B. Any act done or conducted or engaged in by an employee in the course of their employment will be treated as done or engaged in by the employer. This includes volunteers, interns and trainees. However, it is a defense for the employer to prove that it took such steps as were practicable to prevent the employee from doing the act or engaging in the misconduct.

80 In which situation would a data intermediary based in Singapore be liable for breaches against the PDPA?

* A. When it fails to provide an individual access to his or her data.
* B. When it does not provide anonymous transactions with an individual.
* C. When it fails to inform an individual it is processing data from a controller.
* D. When it processes data contrary to the provisions established in the contract.

Under the PDPA, a data intermediary is generally not liable for breaches of data protection obligations if it processes personal data on behalf of and for the purposes of another organization (the data controller) under a contract. However, if the data intermediary processes data in a manner that is contrary to the provisions of the contract, it can be held liable for that breach.

81 In Singapore, a potential employer can collect all of the following data on an individual in the pre-employment phase EXCEPT?

* A. Postings from social media websites.
* B. Information from a background check.
* C. Information about the individual's children.
* D. The individual's university attendance records.

Collecting information about an individual's children is generally not relevant to the employment process and would likely be considered excessive and intrusive under the Personal Data Protection Act (PDPA). Employers should only collect data that is necessary and relevant to the job application process.

NO to C - You can legally collect the rest - A, B &D - B is not relevant for the employment purpose... The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data that are relevant for the purposes, and only for purposes that are reasonable. Consistent with the Notification Obligation, the Purpose Limitation Obligation also limits the purposes for which personal data may be collected, used or disclosed to those which have been informed to the individuals concerned pursuant to the Notification Obligation (where applicable).

A potential employer can collect personal data about an employee (such as A, B and D) for EVALUATIVE purpose, i.e. hiring decision, promotion, continue or terminate their employment, without their consent and without notification.

82 Which of the following is NOT a substantial source of privacy protection for Hong Kong citizens?

* A. The Communications and Surveillance Ordinance.
* B. The Universal Declaration of Human Rights.
* C. The Bill of Rights Ordinance.
* D. The Basic Law.

While the UDHR provides important international principles and standards regarding human rights, including privacy, it is not a legally binding document and does not directly confer legal rights or protections within Hong Kong. In contrast, the Communications and Surveillance Ordinance, the Bill of Rights Ordinance, and the Basic Law provide more direct and enforceable privacy protections within Hong Kong.

Should be B, as Hong Kong is not a signatory to the UDHR. A, C and D are the various constitutional protections of privacy in Hong Kong.

83 Which Hong Kong body has recommended legislation that provides for the right of civil action to be taken when private information is publicly disclosed?

* A. Hong Kong's Court of Final Appeal.
* B. Hong Kong Law Reform Commission.
* C. Office of the Privacy Commissioner for Personal Data.
* D. Standing Committee of the National People's Congress of the PRC.

The Hong Kong Law Reform Commission has made recommendations for legal reforms to provide individuals with the right to take civil action when their private information is disclosed without consent

THE LAW REFORM COMMISSION OF HONG KONG - CIVIL LIABILITY FOR INVASION OF PRIVACY- Chapter 7 Unwarranted publicity given to an individual’s private life Individual privacy may be invaded by unwarranted publicity given to facts concerning an individual’s private life. Giving publicity to intimate information about an individual without his consent can prejudice his ability to maintain social relationships and pursue his career. For instance, publishing the fact that a woman is mentally retarded, a lesbian, a prostitute, a drug addict, a transsexual, illegitimate, a patient receiving treatment for breast cancer, or an attendant in a nightclub may make it difficult for her to maintain a normal relationship with her acquaintances and family members. Thus, an individual may not want others know that he is a prodigy, a subscriber to a philanthropic society, or a wealthy person. Individuals who are grief-stricken and public figures who have suffered a setback are particularly vulnerable to mental distress caused by unwanted publicity.

<https://www.hkreform.gov.hk/en/publications/rprivacy.htm>

84 Which provision of Hong Kong's Personal Data (Privacy) Ordinance (PDPO) strengthens the purpose limitation principle (DPP3)?

* A. Notice; because the data subject must be provided with the purpose of the collection.
* B. Public domain; because the data subjects must agree to the purpose before their information is made publicly available.
* C. Prescribed consent; because the data subject must give express consent to their personal information being used for additional purposes.
* D. Finality; because the purpose for collection of personal information from the subject must be directly related to a function of the collector.

Under DPP3 of the PDPO, personal data must not be used for a new purpose unless the data subject has given prescribed consent. This means that if an organization wishes to use personal data for purposes beyond what was originally stated at the time of collection, they must obtain explicit consent from the data subject. This provision strengthens the purpose limitation principle by ensuring that personal data is only used in ways that the data subject has explicitly agreed to.

DPP3 Use of Data DPP3 prohibits the use of personal data for any new purpose which is not or is unrelated to the original purpose when collecting the data, unless with the data subject’s express and voluntary consent. A data subject can withdraw his/her consent previously given by written notice. Regarding restrictions on use of personal data, Part 6A of the PDPO further requires that data users must obtain informed consent before using a data subject’s personal data for direct marketing or transferring the data to a third party for direct marketing. The consent must be an explicit indication by the data subject and broadly covers an indication of no objection. In other words, silence cannot constitute consent.

This provision ensures that individuals explicitly consent to any additional purposes for which their personal data will be used beyond the original purpose of collection, thus reinforcing the principle of purpose limitation.

85 Based on the model contract released by the Privacy Commissioner for Personal Data (PDPC), Hong Kong, all of the following sections are recommended to be put into a contract to address Ordinance 33 (Data transfer/export) of Hong Kong's Personal Data Privacy Ordinance (PDPO) EXCEPT?

* A. Liability and indemnity.
* B. Exemptions and Definitions.
* C. Termination of the contract.
* D. Obligations of the Transferee.

While "Liability and indemnity," "Termination of the contract," and "Obligations of the Transferee" are critical sections that address various aspects of data protection and responsibilities during data transfer/export, "Exemptions and Definitions" are not typically highlighted as a separate recommended section in the model contract for compliance with Ordinance 33 of the PDPO. The primary focus is on ensuring the clear responsibilities and liabilities of both parties, ensuring compliance, and detailing the obligations of the transferee to protect the transferred data.

Model Contract Below sets out a model contract which may be adapted by parties wishing to transfer personal data outside Hong Kong in accordance with section 33(2)(f) of the Personal Data (Privacy) Ordinance. Applicable law The parties are free to choose the law applicable to the contract between the transferor and transferee. The applicable law should be explicitly stated in the contract. The terms of the model contract are as follows: 1. Obligations of the Transferor 2. Obligations of the Transferee 3. Liability and indemnity 4. Settlement of disputes 5. Termination of the contract

https://www.pcpd.org.hk/english/resources\_centre/publications/guidance/fact1\_model.html A, C and D are all mentioned in the model contract. B is not.

86 In June 2011, the Hong Kong Privacy Commissioner determined that data subject consent is NOT valid if it is what?

* A. Provided by the data subject solely in verbal form.
* B. Used for a directly related but separate purpose.
* C. Bundled with other terms of the agreement.
* D. Intended for direct marketing purposes.

This determination means that consent for the collection, use, or disclosure of personal data must be obtained separately and explicitly and cannot be considered valid if it is simply included as part of general terms and conditions in an agreement. This ensures that individuals are fully aware of and agree to the specific use of their personal data, rather than giving broad consent without proper understanding.

“bundled consent” obtained by the Bank(data controller/data user) cannot be regarded as an express consent, hence falling outside the definition of “prescribed consent”. DPP3 “Personal data shall not, without the "PRESCRIBED" consent of the data subject, be used for any purpose other than- (a) the purpose for which the data were to be used at the time of the collection of the data; or (b) a purpose directly related to the purpose referred to in paragraph (a).”

See paragraph 40: <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R11_7946_e.pdf>

87 Which Indian institution is vested with powers under the Credit Information Companies (Regulation) Act of 2005?

* A. The Reserve Bank of India.
* B. The National Housing Bank.
* C. The Oriental Bank of Commerce.
* D. The Securities and Exchange Board of India.

The Reserve Bank of India (RBI) is responsible for the regulation and oversight of credit information companies in India, ensuring they operate within the framework set by the Credit Information Companies (Regulation) Act of 2005.

Credit Information Companies (Regulation) Act 2005 —In this Act (j) “regulations” means regulations made by the Reserve Bank under this Act; REGISTRATION OF CREDIT INFORMATION COMPANIES 3. Prohibition to commence or carry on business of credit information. —Save as otherwise provided in this Act, no company shall commence or carry on the business of credit information without obtaining a certificate of registration from the Reserve Bank under this Act. 5. Grant of certificate of registration. —(1) The Reserve Bank may, for the purpose of considering the application of a company for grant of a certificate of registration to commence or carry on the business of credit information, require to be satisfied, by an inspection of records or books of such company 6. Power of Reserve Bank to cancel certificate of registration. —(1) The Reserve Bank may cancel a certificate of registration granted to a credit information company

88 Section 43A was amended by India's IT Rules 2011 to include?

* A. A definition of what constitutes reasonable security practices.
* B. A requirement for the creation of a data protection authority.
* C. A list of cases in which privacy policies are not necessary.
* D. A clarification regarding the role of non-automated data.

The amendment introduced the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which provided detailed definitions and guidelines on what constitutes reasonable security practices and procedures for organizations handling sensitive personal data or information.

Section 43A and the 2011 Rules 3-8 In 2011, delegated legislation made under section 43a of the IT Act created a data privacy regime. However, the rules are perhaps ultra vires, apply only to very strict definitions of sensitive data, and provide rights of action only to the “providers of data”. Rule 8: Reasonable Security “Such security practices and standards have a comprehensive documented info sec program and info sec policies that contain managerial, technical, operational, and physical security control measures that are commensurate with the info assets being protected with the nature of business.” “In the event of an info sec breach, the body corporate … shall be required to demonstrate [to agency] that they have implemented security control measures as per their documented info sec program and policies.” Burden of proof in R8 likely does not override 43A’s standard of negligence. But does have separate obligation to demonstrate security.

89 According to India's IT Rules 2011, a body corporate operating in India is required to appoint what kind of authority?

* A. A Chief Risk Officer.
* B. A Grievance Officer.
* C. A Data Protection Officer.
* D. A Chief Technology Officer.

The IT Rules mandate that everybody corporate handling sensitive personal data or information must appoint a Grievance Officer to address complaints and ensure compliance with data protection regulations. The Grievance Officer is responsible for resolving issues related to the processing of personal data and responding to inquiries and complaints from data subjects.

Grievance Officers Required by IT Act 43A and Rule 5(9) Located at company dealing with SPI. Handles any discrepancies and grievances of the provider of info with respect to processing of information in a time bound manner. Must redress within one month.

90 Cases in which an Indian company is accused of violating provisions of India's IT Act must be heard by?

* A. The High Court.
* B. A Grievance Officer.
* C. An Adjudicating Officer.
* D. The Cyber Appellate Tribunal.

The Adjudicating Officer is appointed under the Information Technology Act to adjudicate matters related to contraventions of the Act. They have the authority to handle disputes and impose penalties for violations of the IT Act.

Filing Complaints under IT Act The information technology Act, 2000, specifies the acts which are punishable under the Act. State IT Secretary is the adjudicating officer under the IT Act, to adjudicate matters in respect of contraventions to the Chapter IX of the Information Technology Act 2000 and the matter or matters or places or area/areas in the State in which claim for injury or damage does not exceed Rs. 5 crore. The Adjudicating officer has the powers of Civil Court which are conferred on the Cyber Appellate Tribunal under sub-section(2) of the section 58. Section 46 of The Information Technology Act, 2000 Appointment of Adjudicating Officers: The Indian government will appoint high-ranking officials to investigate and decide if someone has broken the rules of the Information Technology Act or related regulations. These officials must be at least at the level of a Director in the government or an equivalent position in state government.

Cases in which an Indian company is accused of violating provisions of India's IT Act are typically heard by an Adjudicating Officer. Under section 46 of the IT Act, an AO shall be appointed by the Central Government for the purpose of discerning whether or not any person has contravened any provision of the IT Act. The AO is responsible for adjudicating matters related to violations of the IT Act and imposing penalties or fines as necessary.

91 What personal information is considered sensitive in most countries in Asia with such definition in privacy laws?

* A. Financial information.
* B. Health information.
* C. Geolocalization information.
* D. Criminal records.

Health information is typically regarded as sensitive personal data because of its highly private nature and the potential impact on individuals if it is disclosed or misused. Many privacy laws in Asian countries, including India, Singapore, and Hong Kong, include specific protections for health information.

92 The judgement of the Supreme Court in 2017 in the case of Justice K.S. Puttaswamy (retd.) and Anr. vs. Union of India held that?

* A. Right to Privacy is a fundamental right guaranteed by the Constitution.
* B. Right to Privacy is an intrinsic part of Art. 21 of the Constitution.
* C. Right to life and personal liberty includes the right to Privacy.
* D. Right to Privacy is the right to be left alone.

This landmark judgment recognized the right to privacy as a fundamental right protected under the Constitution of India. The Court declared that the right to privacy is intrinsic to the right to life and personal liberty guaranteed under Article 21 of the Constitution.

The Bench unanimously held that “the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution”. In doing so, it overruled previous judgments of the Supreme Court in M.P. The Supreme Court, through six separate opinions, pronounced privacy to be a distinct and independent fundamental right under Article 21 of the Constitution. The crux of the decision spelled out an expansive interpretation of the right to privacy - it was not a narrow right against physical invasion, or a derivative right under Article 21, but one that covered the body and mind, including decisions, choices, information and freedom.

93 In what way are Singapore residents protected following a data breach in ways that India and Hong Kong residents are not?

* A. The affected individuals must be informed when significant harm is likely to occur.
* B. The relevant authority must be informed of such data breach following its discovery.
* C. The company must have in place a data breach response plan including third parties.
* D. The breach must be reported to the relevant authority within 72 hours of the discovery.

Under the Personal Data Protection Act (PDPA) in Singapore, organizations are required to notify affected individuals if a data breach is likely to result in significant harm to them. This requirement ensures that individuals are made aware of breaches that could have a considerable impact on their privacy or security, allowing them to take necessary precautions. While similar provisions exist in some jurisdictions, this specific requirement provides a clear mandate for informing individuals under defined circumstances, offering a distinct layer of protection for Singapore residents.

Singapore - Under the current Act A data breach constitutes a “notifiable data breach” if: it results in, or is likely to result in, significant harm to the affected individuals (including one that compromises personal data prescribed under the Personal Data Protection (Notification of Data Breaches) Regulations 2021); or it is of a significant scale (i.e. one that affects 500 or more individuals). Hongkong - There is no statutory definition of a data breach under the Ordinance. India - “In the event of an info sec breach, the body corporate … shall be required to demonstrate [to agency] that they have implemented security control measures as per their documented info sec program and policies.” Under the DPDP Act, in the event of a personal data breach, Data Fiduciary is required to inform each affected Data Principal

Section 43A of the Information Technology Act, 2000 ("IT Act") required a body corporate that possesses, deals with or handles any "sensitive personal data or information" in a computer resource which it owns, controls or operates, to maintain "reasonable security practices and procedures". The terms "sensitive personal data or information", and "reasonable security practices and procedures" were not sufficiently defined. Exemption For Outsourcing Entities: The obligations under Rules 5 and 6 of the Data Privacy Rules (i.e., relating to the manner in which companies can collect and disclose "sensitive personal data or information") do not apply to Indian companies which collect, store, deal with or handle "sensitive personal data or information" under a contractual obligation with a legal entity.