

IAPP.CIPP-A.by.Jey.54q

Number: CIPP-A  
Passing Score: 800  
Time Limit: 120  
File Version: 3.0

**Exam Code: CIPP-A**



## Exam A

### QUESTION 1

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationgdpr/lawful-basis-for-processing/special-category-data/>

### QUESTION 2

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.



**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en>

### QUESTION 3

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.

**Correct Answer: C**

**Section:**

**Explanation:**

Reference: [http://blog.hawaii.edu/aplpj/files/2011/11/APLPJ\\_04.2\\_chung.pdf](http://blog.hawaii.edu/aplpj/files/2011/11/APLPJ_04.2_chung.pdf)

### QUESTION 4

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:

- A. The recruitment process;
- B. Employee assessment and records management;
- C. 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. Dracarys' 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.

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

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

**Correct Answer: A**

**Section:**

#### QUESTION 5

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.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference: <https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know>

#### QUESTION 6

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.

**Correct Answer: A**

**Section:**

**QUESTION 7**

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.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference: <https://www.burges-salmon.com/news-and-insight/legal-updates/gdpr-personal-data-and-sensitive-personal-data/>

**QUESTION 8**

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.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

<https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f5443a3360c785eab4cc2/1465865429526/china.pdf> (21)

**QUESTION 9**

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.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference: <https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011->

**QUESTION 10**

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.

**Correct Answer: A**

**Section:**

#### QUESTION 11

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.

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://www.casemine.com/judgement/in/5609abd1e4b014971140d6b0>

#### QUESTION 12

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.

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.

**Correct Answer: D**

**Section:**

#### QUESTION 13

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: <https://www.scoobserver.in/reports/k-s-puttaswamy-right-to-privacy-judgment-of-the-court-in-plain-english/#:~:text=On%2024th%20August%2C%202017%20a,a%20fundamental%20right%20to%20privacy>

#### QUESTION 14

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.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference: <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>

#### QUESTION 15

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.

**Correct Answer: A**

**Section:**

#### QUESTION 16

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.

**Correct Answer: C**

**Section:**

**Explanation:**

Reference: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en)

**QUESTION 17**

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.

**Correct Answer: C**

**Section:**

**QUESTION 18**

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.

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.

**Correct Answer: A**

**Section:**

**QUESTION 19**

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.

**Correct Answer: A**

**Section:**

**QUESTION 20**

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.

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011->

#### QUESTION 21

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.

**Correct Answer: C**

**Section:**

#### QUESTION 22

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.

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://www.dataguidance.com/notes/singapore-data-protection-overview>

#### QUESTION 23

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: <https://www.dataguidance.com/notes/singapore-data-protection-overview>

#### QUESTION 24





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.

**Correct Answer: B**

**Section:**

**QUESTION 25**

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.

**Correct Answer: D**

**Section:**

**QUESTION 26**

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.

**Correct Answer: B**

**Section:**

**QUESTION 27**

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.

**Correct Answer: B**

**Section:**

**QUESTION 28**

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.

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.

**Correct Answer: C**

**Section:**

#### QUESTION 29

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.

**Correct Answer: A**

**Section:**

#### QUESTION 30

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: [https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti\\_Money-Laundering\\_Counteracting-the-Financing-of-Terrorism/Guidance-for-Effective-AML-CFT-](https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Counteracting-the-Financing-of-Terrorism/Guidance-for-Effective-AML-CFT-Transaction-Monitoring-Controls.pdf)

Transaction-Monitoring-Controls.pdf (page 3)

#### QUESTION 31

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: [https://en.wikipedia.org/wiki/Information\\_Technology\\_Act,\\_2000](https://en.wikipedia.org/wiki/Information_Technology_Act,_2000)

#### QUESTION 32

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.

**Correct Answer: C**

**Section:**

**Explanation:**

Reference: [https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3204&context=sol\\_research](https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3204&context=sol_research)



#### QUESTION 33

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: [https://www.pcpd.org.hk/english/resources\\_centre/publications/files/GN\\_crossborder\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf)

#### QUESTION 34

What clarification 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.

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://nishithdesai.com/information/news-storage/news-details/article/clarification-to-the-indian-data-protectionlaws.html>

**QUESTION 35**

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.

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediateamendment.html>

**QUESTION 36**

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.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference: [https://www.pcpd.org.hk/english/data\\_privacy\\_law/ordinance\\_at\\_a\\_Glance/ordinance.html](https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html)

**QUESTION 37**

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).

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://ico.org.uk/media/1042349/review-of-eu-dp-directive.pdf>

**QUESTION 38**

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.

**Correct Answer: B**

**Section:**

#### **QUESTION 39**

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.

**Correct Answer: C**

**Section:**

**Explanation:**

Reference: [https://www.pdpc.gov.sg/-/media/Files/PDPC/New\\_DPO\\_Connect/nov\\_15/pdf/Anonymisation.pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/New_DPO_Connect/nov_15/pdf/Anonymisation.pdf)

#### **QUESTION 40**

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.



**Correct Answer: A**

**Section:**

#### **QUESTION 41**

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: <http://www.bareactslive.com/ACA/ACT416.HTM>

#### **QUESTION 42**

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.

**Correct Answer: C**

**Section:**

**Explanation:**

Reference: <https://www.mondaq.com/india/data-protection/626190/information-technology-reasonable-security-practicesand-procedures-and-sensitive-personal-data-or-information-rules-2011>

#### QUESTION 43

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.

**Correct Answer: C**

**Section:**

#### QUESTION 44

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: <https://www.cpomagazine.com/data-privacy/direct-marketing-hong-kong-summary-key-privacy-issues/>

#### QUESTION 45

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

- A. Financial information.
- B. Health information.
- C. Geolocation information.
- D. Criminal records.

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://www.refworld.org/pdfid/5643021b4.pdf>

**QUESTION 46**

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.

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.

**Correct Answer: C**

**Section:**

**QUESTION 47**

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.

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.

**Correct Answer: D**

**Section:**

**QUESTION 48**

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.

**Correct Answer: C**

**Section:**

**Explanation:**

Reference: [https://www.pcpd.org.hk/english/publications/files/GN\\_DM\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf)

#### QUESTION 49

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.

**Correct Answer: D**

**Section:**

**Explanation:**

Reference: <https://cic.gov.in/sites/default/files/Section%20of%20the%20RTI%20Act%20-%20Ankur%20Mishra.pdf> (9)

#### QUESTION 50

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.

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.

**Correct Answer: B**

**Section:**

#### QUESTION 51

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.

**Correct Answer: B**

**Section:**

#### QUESTION 52

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.

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.



**Correct Answer: D**

**Section:**

#### QUESTION 53

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: [https://tahseen.ae/media/3481/india\\_information-technology-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.pdf](https://tahseen.ae/media/3481/india_information-technology-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.pdf)

#### QUESTION 54

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.

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.

**Correct Answer: B**

**Section:**

